Egovernment
elektronizace veřejné správy

DIAGNÓZA TRANSFORMACE

Egovernment

elektronizace veřejné správy

Vše o elektronizaci veřejné správy - srozumitelně a zdarma:

www.egovernment.cz

DOKTOR IVAN A JEHO LÉK

Hovořit o českém e-governmentu je tak trochu jako točit se v bludném kruhu. Každoročně prezentujeme realizované kroky, vykonanou práci, nastavené projekty ... grafy, cifry, pochvaly. A pak se dočkáme pravidelného mezinárodního srovnání a místo očekávaného posunu v žebříčku pozorovaných zemí směrem nahoru, zaznamenáme pokles. A zase, ubezpečíme se, že tentokráte to bylo naposledy, protože teď už, konečně, se začne naše dosavadní práce zúročovat. A tak prezentujeme vykonanou práci a nastavení projektů ... abychom se opět dočkali poklesu. A zas a znova. Letos konkrétně jsme v hodnocení DESI – Digital Economy and Society Index, nebo chcete-li index digitální ekonomiky a společnosti, takto sklesali na 19. příčku z 27. To se již nedá hodnotit ani jako průměr, ale skutečně umístění pod průměrem. Za námi se nachází Kypr, Chorvatsko, Maďarsko, Slovensko, Polsko, Řecko, Bulharsko a Rumunsko. Všichni ostatní jsou před námi.

Je tedy zřejmé, že náš tradiční přístup na udržení pozic nestačí, a pokud chceme pomýšlet na posun směrem nahoru, což podle každoročního vyjádření odpovědných chceme, bylo by třeba radikálního řezu. I proto přichází „Doktor Ivan" se svým návrhem **transformace koordinace a řízení digitalizace**, jehož nejviditelnějším a patrně nejdiskutovatelnějším bodem je **DIA – digitální informační agentura**. Jak sám místopředseda vlády, odpovědný za digitalizaci, uvádí, jsou státy (jako například Dánsko), které mají takové agentury až čtyři. Nám prý bude stačit jedna. Pravda, má to svoje úskalí, je potřeba delimitovat, modernizovat, definovat a stabilizovat. Ale prý se to všechno povede.

Výsledkem „léčby" by měla být situace, kdy digitalizace státu bude koordinována z jednoho bodu, který vlastně bude podřízen přímo premiérovi. Mělo by to být tím pádem nezávislé na jednotlivých resortech i politicích, přehledné a funkční. Co přesně v sobě transformace zahrnuje a jak je rozfázována, se můžete dočíst na následujících stranách. Jak moc bude účinná, si povíme třeba už za rok, až budeme v Mikulově diskutovat nad naší pozicí v evropském hodnocení roku 2023. Snad to nebude jen další otáčka v onom bludném kruhu.

Pěkné čtení

Michal Jirkovský,
šéfredaktor

Obsah

V rámci České a Slovenské republiky vydává:
info◆com s.r.o, Na Zatlance 10, 150 00 Praha 5
www.infocom.cz
IČO: 26426331
zapsána u Městského soudu v Praze
pod č. C – 81357
tel.: 241 412 518
e-mail: egovernment@egovernment.cz
http: www.egovernment.cz
twitter: @EgovernmentMag
facebook: @EgovernmentMagazin

Šéfredaktor: Ing. Michal Jirkovský
Korektorka: PhDr. Helena Veverková
Asistentka: Karolína Modranská

Grafika: PROPAGANDA, Malá Štupartská 7, Praha 1
Tiskárna: A. R. GARAMOND s.r.o., Belnická 758, 252 42 Jesenice
Registrační číslo: MK ČR E 11364
ISSN 1801-9420

Registrace:

Magazín Egovernment je distribuován, na základě registrace, pracovníkům veřejné správy v České republice a na Slovensku **ZDARMA**.
Ostatní čtenáři, kteří nejsou pracovníky veřejné správy zaplatí cenu **300 Kč** bez DPH**/výtisk, tj. 900 Kč** bez DPH **ročně**.
S registrací získáte, kromě pravidelného zasílání magazínu, i informace o dalších projektech, které realizuje společnost **info◆com** s.r.o.

INFORMAČNÍ SYSTÉMY ICZ VÁM DODAJÍ JISTOTU A STABILITU

S NÁMI JSTE **SILNĚJŠÍ!**

[ZDRAVOTNICTVÍ]

[VEŘEJNÁ SPRÁVA]

[INFRASTRUKTURA]

[ŘÍZENÍ LETOVÉHO PROVOZU]

[OBRANA]

[BANKOVNICTVÍ A POJIŠŤOVNICTVÍ]

[BEZPEČNOST]

[LOGISTIKA]

[ŘÍZENÍ LETOVÉHO PROVOZU]

www.iczgroup.com

MIKULOV 2022

Magazín Egovernment uspořádal letos již 14. ročník konference zaměřené na elektronizaci veřejné správy pod názvem e-government 20:10, aneb žijeme si jak na zámku, ať to trvá věčně. Letošní ročník byl po dvou „covidových" opět „normálním" a to si jak účastníci, tak vystupující s chutí užili. Kapacitu mikulovského zámku jsme díky tomu letos otestovali na jeho maximální hranici, stejně jako „propustnost" programu. Počet prezentací byl takový, že jsme poprvé v historii konference museli zkracovat obědovou přestávku, aby se stihla všechna vystoupení.

Maximální účast byla znát už u registrace, když v době zahajovacích proslovů se ještě přes nádvoří táhla fronta neodbavených účastníků sledující úvodní projevy na svých mobilních telefonech. Bohatý program, krásné počasí a odpočinková zóna na terase vedle zámeckého sálu s krásným výhledem na Svatý kopeček jim ranní nepohodlí následně dostatečně vynahradilo.

I letos se konference konala pod záštitou starosty města Mikulov Rostislava Koštiala, hejtmana Jihomoravského kraje Jana Grolicha, ministra vnitra a prvního místopředsedy vlády Víta Rakušana a místopředsedy vlády pro digitalizaci Ivana Bartoše. A tak přímo oni či jejich „zmocněnci", kterými byli radní pro vědu, výzkum a informatiku Jihomoravského kraje Jiří Hlavenka a náměstek člena vlády Lukáš Kolařík, přivítali přítomné v sále i doma či v kancelářích při sledování streamu. Ministerstvo vnitra pak v tradiční pasáži přiblížilo současný stav e-governmentu ve vystoupeních Petra Kuchaře, ředitele odboru hlavního architekta, a Michala Peška, ředitele SZR. Celý blok uvedl poněkud netradičně videovstupem ze Svatého kopečku Roman Vrba, ředitel odboru eGovernmentu, a na něj navázal David Sláma, pověřený řízením sekce veřejné správy a eGovernmentu MV ČR.

Samostatnou součástí tohoto odborného úvodu konference byla praktická ukázka eSEL. Elektronická sbírka a elektronická legislativa jsou projekty, o kterých se velice, opravdu velice dlouho hovoří, ale hmatatelné výsledky nebyly stále k dispozici. I proto úvodní slide této prezentace a ukázky zároveň přibližovaly eSEL jako sněžného muže **Yettiho**, neboť i o něm se stále mluví, ale nikdo jej skutečně ještě neviděl. David Sláma přiblížil historii eSEL a následně předal slovo svým kolegům. Především náměstek ministra vnitra pro řízení sekce legislativy a veřejné správy Petr Vokáč a prezident ICT Unie Zdeněk Zajíček přehledným a srozumitelným způsobem ukázali, co se podařilo v projektu eSEL již realizovat a jak vlastně funguje. V živé ukázce předvedli tvorbu, připomínkování a přijímání návrhů zákonů, jak by mohly díky tomuto nástroji fungovat.

Prezentace jsme následně přerušili diskuzemi. V rámci konference jsme přímo na podiu uspořádali **Studio Egovernment**, tedy stream odborných diskuzí na aktuální témata. Jako prvního hosta jsme si pozvali vicepremiéra pro digitalizaci Ivana Bartoše a probrali s ním vládní návrh transformace koordinace a řízení digitalizace, jehož stěžejním bodem je zřízení **Digitální informační agentury** (str. 14). Následně jsme k němu na pódium přizvali Petra Kuchaře, ředitele odboru hlavního architekta, Tomáše Hebelku, generálního ředitele Státní tiskárny cenin, Jana Blažka, předsedu představenstva BankID, a právníka Jana Tomíška za Rowan Legal. Tématem jejich debaty bylo **eIDAS 2.0**, tedy elektronická peněženka, kterou navrhuje EU. Pokud Vás zajímá, k čemu a odkdy bude sloužit, jak či zda se může 27 elektronických peněženek spolu dohodnout, pak se podívejte na stranu 22.

S Tomášem Šedivcem z ministerstva vnitra jsme se následně vrátili k architektuře e-governmentu. Informoval nás o aktualitách Národního architektonického plánu. A jako zajímavost jsme zařadili vystoupení platinového partnera konference, společnosti CISCO. Jaroslav Martan přiblížil komunikační technologie při našem předsednictví EU a rovněž ukázal, jak video může být komunikačním prostředkem občanů s Policií ČR (str. 18).

Celý dopolední program konference uzavírala debata s novým ředitelem Národního úřadu pro kybernetickou a informační bezpečnost Lukášem Kintrem. Kromě jeho reakcí na předchozí informace o některých projektech a jeho kyberbezpečnostní pohled byla hlavním tématem směrnice NIS2, tedy rozšíření „záběru" zákona o kybernetické bezpečnosti (str. 26).

Po tomto úvodním „nášupu" jsme všichni odběhli na oběd, ale jak bylo řečeno, ti, kteří chtěli sledovat sekci Egovernment, si museli pospíšit.

Odpolední program se rozdělil do dvou sekcí. Kromě Egovernmentu, kterému byl věnován zámecký sál, probíhaly prezentace v Bezpečné kavárně. Tady jsme se zaměřili na kyberbezpečnost. V obou sekcích se jednalo o sled jednotlivých prezentací, který již nebyl přerušen žádnou diskuzí a končil kolem šesté odpolední.

Mezitím byl v nástupním sále připraven raut pro všechny účastníky konference a na zámeckém nádvoří instalována aparatura a světelná technika k vystoupení kapely **B.LUES**. Ta spustila ve 20:00 a dvě hodiny doslova žhavila naše konferenční publikum. S naprostou jistotou odehrála trháky od Pink Floyd, Stinga či Tiny Turner a dalších světových interpretů a rozpohybovala všechny přítomné. Úspěch byl takový, že diváci, posluchači a tanečníci současně rozhodně nechtěli B.LUES jen tak propustit a vynutili si několikerý přídavek. Útěchou jim pak mohla být diskotéka pod hvězdami na zámeckém nádvoří, která končila až s půlnocí.

Druhý konferenční den je tradičně věnován uvolněnější formě, tedy jakémusi workshopu. Pro něj jsme letos zvolili téma **kyberbezpečnost ve zdravotnictví** a pozvali k diskuzi Víta Lidinského, manažera kybernetické bezpečnosti z Ministerstva zdravotnictví, Petra Pavlince, vedoucího odboru informatiky z Kraje Vysočina, Adama Kučínského, ředitele odboru regulace Národního úřadu pro kybernetickou a informační bezpečnost, a Jana Koloucha, metodika kybernetické bezpečnosti CESNET. Jejich názory byly proloženy prezentacemi odborníků ze společností F5 a Fortinet se zaměřením právě na problematiku bezpečnosti zdravotnictví.

I díky krásnému počasí, množství prezentací a velké návštěvnosti patří letošní ročník konference e-government 20:10 k těm nejúspěšnějším. Vy si na následujících stránkách můžete přečíst jak informace o některých vystoupeních, tak názory a články, které byly reakcí na tato vystoupení. A my mezitím už začínáme připravovat další ročník.

Jednotlivé prezentace, videa z vystoupení a diskuzí i fotogalerii z konference naleznete na www.egovernment.cz v sekci Mikulov 2022.

e-government 20:10

aneb žijem si jak na zámku, ať to trvá věčně

MIKULOV • 6. – 7. 9. 2022

Nebyli jste na konferenci v Mikulově a chtěli byste vidět některá z vystoupení?

www.egovernment.cz

V sekci Mikulov najdete odkazy na PDF verze prezentací, videozáznamy jednotlivých vystoupení i kompletní fotogalerii.

e-GOVERNMENT AKTUÁLNĚ A PŘEHLEDNĚ

Úvod bloku za celé MV ČR obstaral Roman Vrba, ředitel odboru eGovernment MV ČR, který sice nemohl z pracovních důvodů dorazit na samotnou konferenci, přesto nás pozdravil přímo z Mikulova. O víkendu, který konferenci předcházel, vyběhl na Svatý kopeček a natočil krátké přivítání. V něm především upozornil na důležité změny v oblasti datových schránek k 1. 1. 2023, které je možné sledovat na chcidatovku.gov.cz a jimž se rovněž ve svém vystoupení bude věnovat Andrea Barešová z České pošty. Dále avizoval vystoupení Jana Kaliny z odboru eGovernmentu, který uvede novinky v rámci Portálu občana. Roman Vrba přitom vidí jako nejzajímavější tu skutečnost, že se do Portálu nyní můžete dostat pouze na jedno kliknutí. Posledním tématem a prezentací, na kterou diváky svého videopříspěvku Roman Vrba upozornil, byl vstup Filipa Bílka k tématu eIDAS2.0

Další zástupci MV ČR už byli fyzicky přítomni v zámeckém sále. Jako první v pořadí se slova ujal **David Sláma**, který je pověřen řízením sekce veřejné správy a eGovernmentu. Ten za velice důležité téma současnosti považuje práci s daty. I proto upozornil na skutečnost, že MV ČR připravuje do meziresortního připomínkového řízení věcný záměr zákona o správě dat, neboť si na MV jsou vědomi toho, jakým způsobem je v současné době v ČR omezeno právě nakládání s daty. Je to podle jeho mínění téma, které si zaslouží pozornost tak, aby pro účely veřejné správy byla data daleko více k dispozici. Ministerstvo vnitra v této souvislosti připravuje na podzim školení pro analytiky, a to na všech úrovních státní správy a samosprávy.

V další části David Sláma uvedl vystoupení některých svých kolegů. Tématem, které je nyní rovněž velice důležité, je Národní katalog otevřených dat – o tom bude podrobněji hovořit Petr Kuchař. Proto David Sláma jen zdůraznil, že v roce 2022 se díky legislativním úpravám podařilo navýšit počet poskytovatelů otevřených datových sad (nyní je to cca 260 poskytovatelů). 10 milionů identitních prostředků a nápor na NIA jsou fakta, která bude rozebírat Michal Pešek. David Sláma jako zásadní vidí skutečnost, že 16 % obyvatel se alespoň jednou přihlásilo k digitální identitě nejrůznějšími prostředky. To není rozhodně špatné číslo. V porovnání s ostatními zeměmi se tak nacházíme v té „lepší“ polovině.

Za zmínku považoval David Sláma vhodné rozhodně skutečnost, že od letošního roku je k dispozici portál sbírky právních předpisů územněsamosprávních celků. Podstatné je, že se k němu přihlásilo velké množství samospráv. Zpřístupnily tak široké veřejnosti obecně závazné vyhlášky - svoje právní regulace. Momentálně je lídrem v tomto směru Brno, které do portálu nahrálo už 150 právních předpisů. Celkově je zde k dohledání 11,5 tisíce dokumentů v podobě nařízení, vyhlášek. Podle Davida Slámy se jedná o nástroj, který rozhodně posílil přístup k právu. Dalším takovým projektem je elektronická sbírka a elektronická legislativa, tedy projekt eSEL, který bude představen podrobněji.

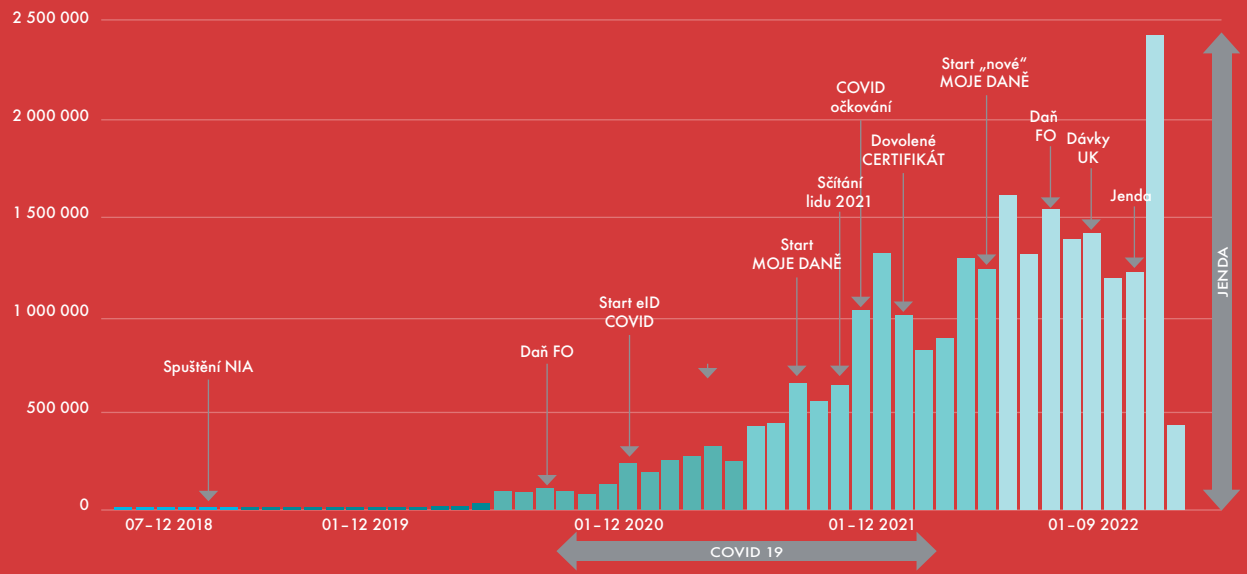
Petr Kuchař, ředitel odboru hlavního architekta MV ČR, navázal prezentací aktualit z centra koordinace eGovernmentu. Na pomoc si vzal základní čísla o rozvoji identitního prostoru:

- celkový počet identitních prostředků nyní činí 10 174 122 (to znamená, že někteří mají i vícero identitních prostředků);
- počet občanů disponujících alespoň jedním prostředkem je 5 513 485;
- z tohoto počtu se alespoň jednou přihlásilo 1 799 473 osob.

Petr Kuchař zdůraznil, že určitými premianty v agendě elektronické identifikace jsme se stali díky BankID, i když nejoblíbenějším prostředkem přihlášení zůstává NIA ID (jméno, heslo, SMS) a činí 6,2 mil. přihlášení. Druhým v pořadí je mobilní klíč e-governmentu (4 mil.).

Z nabízené bankovní identity je nejvíce využívaná Česká spořitelna, která registrovala v NIA 2,1 mil. prostředků.

KLÍČOVÉ MOMENTY DLE PŘIHLÁŠENÍ



SLUŽBY

Nejžádanějšími službami jsou IS DS, ePortál ČSSZ, Ústav zdravotnických informací. Petr Kuchař ale upozornil na aplikaci Jenda, klientský portál MPSV. Celkově bylo za celý srpen ke službám státu evidováno 2,444 mil. přihlášení (žádostí o elektronickou identifikaci). Z toho, především v souvislosti s jednorázovým příspěvkem na dítě, 1,11 mil. k portálu Jenda. Ten je přitom k dispozici od 15. 8. a poslední dva týdny došlo k nárůstu provozu NIA o 200 %.

Jak je vidět z grafu, přihlašování rozběhla problematika covidu, dále pak postupně agendy moje daně, sčítání lidu, dávky ukrajinským běžencům a nyní zmiňovaný portál Jenda. Právě z jeho náběhu vyplynulo podle slov Petra Kuchaře určité poučení – NIA jako taková kapacitní problémy nemá, je vyladěná a stabilní. Máme ale podfinancovány základní registry (v tomto případě ROB a ISZR), které se podílejí na dodávce dat do NIA.

Proto 15. 8., kdy odstartoval portál Jenda, neúnosně vznikaly prodlevy pro dodávku dat. To je oblast, do které bude podle jeho slov nutné investovat. A samozřejmě se ukázalo, že případné hromadné odstávky je nutno lépe koordinovat. Stává se, že při množství odstávek v tom „vláčku" návazných prvků se ruší systémy, které mají fungovat 24/7.

Jako poslední k NIA Petr Kuchař uvedl, že naše mezinárodní gateway je nyní propojena se všemi státy, s nimiž je to aktuálně možné. V případě Lichtenštejnska probíhá notifikace a doposud není možné propojení s Irskem, Islandem, Maďarskem, Bulharskem a Rumunskem.

OTEVŘENÁ DATA

Petr Kuchař přivítal, že se povedlo zvýšit počet subjektů v Národním katalogu ověřených dat, tedy oněch publikujících (z 53 na 260 poskytovatelů). K tomu došlo v důsledku legislativní úpravy, která byla součástí DEPO, do kterého se dostal poslanecký návrh, jenž nařizuje v rámci otevřených dat zveřejňovat úřední desky. Petr Kuchař očekává další výrazný nárůst poskytovatelů otevřených dat díky prováděcímu aktu EK, který nařizuje zveřejňovat v Katalogu i data s tzv. vysokou socioekonomickou hodnotou. Je však smutnou pravdou, že nám chybí datoví specialisté. Krom toho často nevíme, jaká data se v rámci VS sbírají, co znamenají a kde je možné je najít. To je podle Petra Kuchaře velký prostor na zlepšení.

INFORMAČNÍ SYSTÉM SDÍLENÉ SLUŽBY

(původně eGSV – eGon Service Bus)

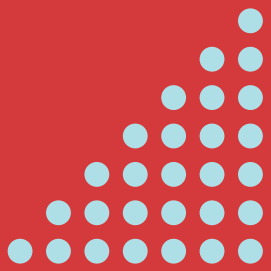
V této problematice dochází k rozložení mezi MV (OHA), který bude činit architektonický dohled, a věcným správcem, jímž je nyní SZR. Jedná se o agendový přenos XXML dat, který slouží orgánům veřejné moci a není určen občanům. V současné době je dokončováno převzetí SZR a určitá technická zlepšení. Petr Kuchař toto vystoupení zakončil jen zdůrazněním, že pro OHA je při schvalování výdajů na ICT velice důležitá otázka, jaká data OVM z agendy zveřejňuje, resp. proč, s tím, že tlak na publikaci dat bude rozhodně výrazně rozšířen.

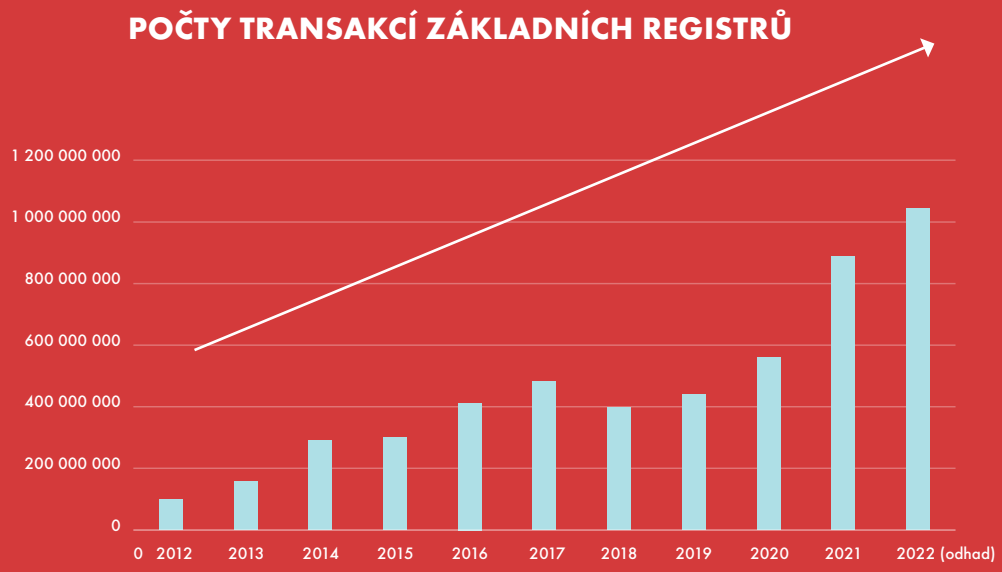
Michal Pešek, ředitel Správy základních registrů, byl třetím v pořadí v tomto tradičním bloku. Chce se věnovat jak Národní identitní autoritě (elektronická identifikace), tak Informačnímu systému sdílené služby a rád by, aby to bylo vnímáno jako určitý apel na to, aby centrální správa začala více publikovat e-služby tak, aby občané stále nemuseli dokládat to, co je již k dispozici.

DESET LET

Michal Pešek připomenul, že je to přesně deset let od spuštění základních registrů, a tak je možná dobré se podívat na systém očima čísel:

- od 1. 7. 2012 do 1. 7. 2022 proběhly 4,3 miliardy transakcí;
- od 1. 1. 2022 do 1. 9. 2022 680 milionů transakcí;
- za poslední týden 23 milionů;
- denně 3–4 mil. transakcí.





Tento náběh vytížení je podle Michala Peška základním problémem, neboť se odehrává na stále stejné infrastruktuře. Přitom neskutečně narostlo vytížení, proto je na místě diskuze o jisté obnově a posílení systému základních registrů.(Pro představu, co ta čísla znamenají, probíhá ve špičkách v průměru 53 transakcí za sekundu, nárazově pak 190 až 250.)

Pokud jde o Informační systém sdílené služby – eGon Service Bus, nejviditelnější bude zřejmě příprava přístupového portálu, který OVM zjednoduší připojení k těm systémům. Jednotlivé činnosti jsou rozděleny mezi MV, Nakit a SZR, konkrétní informace jsou k dispozici na těchto odkazech - QR. Samotný portál bude k dispozici od 1. 1. 2023.

NIA

Pro NIA byly hlavní milníky:

- v roce 2016 nařízení eIDAS;
- v roce 2018 zákon o elektronické identifikaci;
- v roce 2021 BankID.

Výsledkem je skutečnost, že k 5. 9. 2022 bylo:

- 10,15 mil. vydaných prostředků (90 % nestátních);
- 5,5 mil. s jedním aktivním prostředkem;
- 1,7 mil. unikátních uživatelů, kteří identitu využili.

Nejčastěji je využíváno připojení k těmto službám:

- Portál občana;
- ÚZIS – očko portál, tečka;
- sčítání lidu 2021;
- nouzový stav – covid programy;
- služby pro ministerstvo dopravy (STK, mýtné, ŘP);
- ČÚZK – nahlížení do katastru;
- ČSSZ služby;
- Daňový portál.

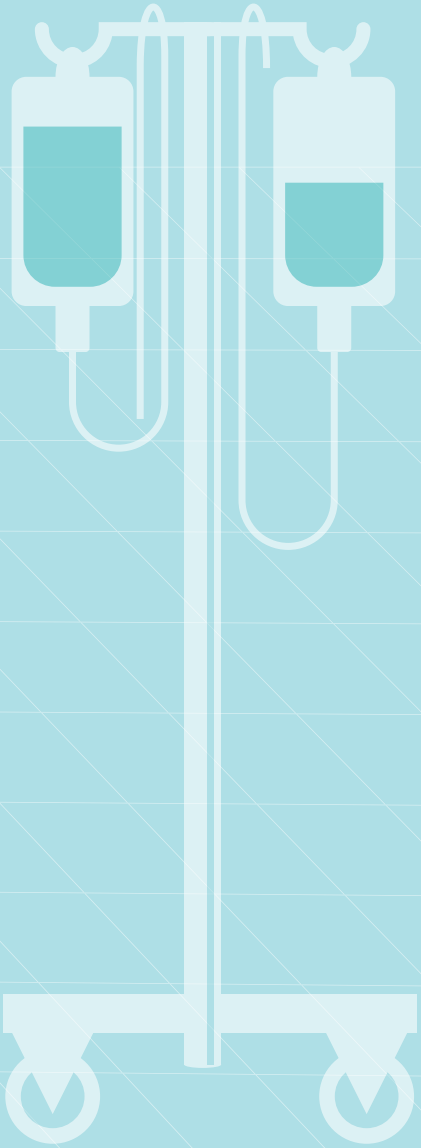
ROZVOJ NIA V ROCE 2022

Michal Pešek upozornil, že je tedy velice nutné věnovat pozornost dalšímu rozvoji NIA. Nyní bude dalším podstatným momentem zřízení datové schránky při prvním použití identifikačního prostředku (účinnost od 1. 1. 2023), dále pak postupná náhrada rodného čísla v komunikaci se subjekty za BSI, služby autorizace digitálního úkonu a zahájení změn na portálu Národního bodu směrem ke zvýšení uživatelské přívětivosti. Podstatné podle jeho mínění je, aby pro zvýšení dostupnosti a výkonnosti proběhly zásadní změny na pozadí celého Národního bodu.

Michal Jirkovský

NOVÁ KREV DO ŽIL eGONA?

Patrně nejvíce sledovaným tématem současnosti v oblasti elektronizace veřejné správy v ČR je „transformace koordinace a řízení digitalizace", tedy vládní záměr na úpravy kompetencí a především vznik Digitální informační agentury (DIA). Zájem o toto téma potvrdilo i hlasování v úvodu konference, kdy v „soutěži" s ostatními možnými tématy byla DIA tou nejvíce žádanou. I proto k diskuznímu stolku na podiu usedl Ivan Bartoš, vicepremiér pro digitalizaci, aby tento záměr, který vládě předkládal, blíže vysvětlil, případně odpověděl na dotazy přítomných.



RYCHLÝ, VLÁDNÍ, NESTADARDNÍ

Poslanecká sněmovna v současné chvíli projednává jako sněmovní tisk č. 287 návrh novely zákona o právu na digitální služby. Právě novelizace tohoto zákona by měla zajistit vznik nové instituce, kterou je Digitální informační agentura. Ta by měla de-facto převzít koordinační roli budování a provozování e-governmentu v České republice. Určitá nestandardnost projednávání se projevila už v rámci meziresortního připomínkového řízení tohoto návrhu, které proběhlo ve zkrácené lhůtě a s redukovaným počtem dotčených orgánů. I tak se objevily připomínky MV ČR i MF ČR, ale vzhledem k tomu, že návrh vycházel z programového prohlášení vlády, byl i přes tyto výhrady vládou v polovině srpna schválen.

Do Sněmovny tedy návrh dorazil ještě koncem prázdnin, bylo mu přiděleno, jak už řečeno, číslo 287 a poslanci jej projednali v prvém čtení na počátku září. Vlastně jeho projednávání připadlo přímo na stejný den, kdy se konala naše konference v Mikulově. I proto jsme museli na poslední chvíli upravovat program tak, aby vicepremiér mohl odjet a být včas ve Sněmovně. Další nestandardnost spo-

čívala v požadavku Ivana Bartoše, aby Sněmovna přijala tento návrh již v rámci prvního čtení, a to v předložené podobě bez jakýchkoliv změn. Poslanci mu však nevyhověli a materiál postoupili do obvyklého procesu tří jednání s možností pozměňovacích návrhů, nicméně respektovali alespoň jeho požadavek na zkrácení lhůty pro projednávání ve výborech (na 30 dní). Znamená to tedy, že druhé čtení návrhu tohoto zákona může proběhnout nejdříve v polovině října. Samozřejmě nyní také bude záležet i na výsledcích voleb a celkové politické situaci. I proto se objevují kritické připomínky, které varují, že není zcela reálné přijmout zákon, který by skutečně umožňoval, aby Digitální informační agentura vznikla k 1. 1. 2023.

NENÍ TO APRÍL

Ivan Bartoš v rámci diskuze v Mikulově vysvětloval, že současná situace v rámci elektronizace veřejné správy v ČR dozrála do stadia, kdy je potřeba vytvořit určitou politicky rezistentní autoritu, která na jedné straně dokáže poskytovat expertní pomoc například s implementací, dokáže ale rovněž zajistit přenos know-how mezi jednotlivými resorty a zároveň řídit základ e-governmentu, kterým jsou základní registry a identifikační nástroje. Jak dále uvedl, vzor pro tento postup si vláda vzala ze států s vyspělým e-governmentem, jako jsou Estonsko, Velká Británie či Dánsko. To například, jak Ivan Bartoš zdůraznil, má hned čtyři takové agentury (jedna je srovnatelná s tím, co by měla zajišťovat naše DIA, tedy se věnuje standardům a nadresortním projektům, další pak zajišťuje kompletní IT podporu pro všechny resorty, třetí je zaměřena na nákupy - veřejné soutěže - a poslední pak řeší personální problematiku). Nám by podle slov Ivana Bartoše měla stačit jedna agentura – DIA. Fungovat by měla už příští rok, konkrétně od 1. 4. 2023. A není to apríl, přestože je nutné upravit do té doby řadu zákonů, obstarat dost peněz, přesunout velké množství lidí a hodně nových přijmout.

PENÍZE BUDOU?

Jak bylo řečeno, výhrady k návrhu mělo mimo jiné i MF, které nechce poskytovat další finanční prostředky. Konkrétně „trvá na tom, aby se neinvestovalo do dalšího úřadu s větším počtem zaměstnanců, digitální transformace se má provést se stejným či menším počtem pracovníků, kteří se e-governmentem zabývají nyní." Vicepremiér Bartoš považuje takový postoj vůči jakémukoliv požadavku na další navyšování čerpání z rozpočtu za logický, nicméně se domnívá, že s ohledem na rozsah „pouhých" 300 mil. Kč ročně se pro tento účel podaří peníze zajistit. Část by přitom měla být pokryta v rámci Národního plánu obnovy. Ivan Bartoš navíc zdůraznil, že konkrétně v příštím roce se bude jednat o plynulý náběh jak samotné agentury, tak jejích finančních potřeb. I proto je v otázce zajištění finančních prostředků optimistou.

A PERSONÁL?

Optimistický je Ivan Bartoš i v otázce zajišťování personálu DIA. V rámci návrhu zákona by měli být delimitováni někteří odborníci z MV (OHA a odbor eGOV), ale bude potřeba rovněž přilákat nové. Těm je Ivan Bartoš připraven nabídnout výhodnější podmínky mimotarifního zařazení. Nespecifikoval blíže, jakým způsobem by vedle sebe agentura postavila zaměstnance pod služebním zákonem přicházejícím z MV (tarifní třídy) a tyto nové experty. Uvedl jen, že by se mohlo jednat i o čerstvé absolventy, pro které by to mohla být zajímavá

startovací zkušenost do profesního života. Otázkou je, zda bude skutečně tolik expertů k dispozici, jak si Ivan Bartoš představuje, neboť v souvislosti se směrnicí NIS2 dojde k výraznému rozšíření dopadu KYBEZ zákona až na 6000 „nových" organizací. Je tedy velice pravděpodobné, že tyto „nově" zařazené organizace budou rovněž shánět experty v oboru informačních technologií. Rozhodně bude tedy převis nabídky pracovních příležitostí v tomto oboru v rámci veřejné správy.

AGENTURA

Nový úřad nebude ministerstvem. Návrh zákona jej definuje jako agenturu. Podle Ivana Bartoše je určitým příkladem pro model takové agentury například NÚKIB, který se postupně profiloval jako organizace s mezinárodním kreditem, jež má sílu stanovovat standardy v dané oblasti a přitom je nezávislá na momentálním sestavení vlády. Přesně tak by měla být podle jeho mínění realizována DIA.

I když vznik určité apolitické autority podřízené premiérovi (či vicepremiérovi) dává smysl, kritizováno je rovněž rozdělení kompetencí. Jak bylo řečeno, části odborů z MV (konkrétně odboru hlavního architekta a odboru eGovernmentu) by se měly přesunout do této nové agentury. Tím by ale došlo k oddělení elektronizace od procesů, což je předmětem části kritiky. Jejich spojení bylo totiž nespornou výhodou umístění e-governmentu na MV ČR. Kritikům transformace, má-li proběhnout v uvedeném rozsahu, rovněž vadí počet „zasažených" zákonů, které bude potřeba upravit. Jedná se minimálně o služební zákon, kompetenční zákon, zákon o státním rozpočtu, základních registrech, o ISVS či o elektronických úkonech a autorizované konverzi. Vicepremiér pro digitalizaci však tvrdí, že po legislativní stránce je vše pečlivě připraveno, a co se týče výsledku, je optimistický. Digitální informační agentura vznikne! Není podle něj podstatné, jestli skutečně začne pracovat 1. 4. 2023, nebo s nějakým mírným zpožděním.

CO ZNAMENÁ TRANSFORMACE

Doposud jsme hovořili o momentálně nejviditelnějším a nejdiskutovanějším bodu celé uvažované transformace. Jejím výsledkem, tak jak si ji vláda schválila, by měly být i další kroky:

1. vznik sekce pro digitalizaci a digitální transformaci (pod úřadem vlády);
2. vznik Digitální informační agentury – vznikne transformací SZR a delimitací některých útvarů MV. Ročně bude potřeba cca 300 mil. Kč. Dojde k vytvoření 128 nových pracovních míst, přesunu 187 stávajících pracovníků z jiných úřadů;
3. vznikne Národní datové centrum;
4. dojde ke změnám v rámci SPCSS a NAKIT.

HARMONOGRAM

- **Specifikace zadání pro právní úpravu** – do 15. 3. 2022
- **Zpracování návrhu právní úpravy** – do 15. 4. 2022
- **Předložení právní úpravy vládě** – do 1. 5. 2022
- **Předložení právní úpravy Poslanecké sněmovně** – do 15. 5. 2022
- **Projednání právní úpravy ve sněmovně** – do 30. 9. 2022
- **Projednání právní úpravy Senátem** – do 15. 11. 2022
- **Nabytí účinnosti právní úpravy** – 1. 1. 2023

Microsoft

Digitální úřad

Už dnes existuje celá řada připravených digitálních řešení, která zefektivní chod úřadů a umožní poskytovat kvalitní služby občanům. Prostřednictvím internetu si můžeme zajít třeba do banky nebo supermarketu – je tak na čase, abychom takové možnosti nabídli i v prostředí veřejné správy.

Inspirujte se na digitalni-urad.cz

Shape the Future
Czech Republic

Odborní garanti

Městská část Praha 5 · digitální Česko · NAKIT · Microsoft

Partneři projektu

SOITRON · Principal · NAKIT · feedyou · pwc · Reservatic · CGI · Unicorn · mainstream · Cleverlance · simac · predú · mluvii · Grant Thornton · DATRON · trask · 602 · Power BI · EXPIN IT · ALVAO · DEV:G · Surface · ADASTRA · S&T

Policejní Pol Pointy ve Středočeském kraji jsou úspěšným příkladem digitalizace

Ve Středočeském kraji vznikají další a další Pol Pointy. Už jich je celkem 30.

Středočeský kraj jde v otázce digitalizace služeb veřejnosti příkladem. Právě v tomto kraji je totiž nejvíce kontaktních míst, odkud mohou lidé podávat oznámení Policii ČR videokonferenčně. Jde o nejrychlejší způsob, jak podat trestní oznámení nebo ohlásit protiprávní jednání. Eliminuje překážky, kvůli nimž se lidé někdy na policii zdráhají obrátit. Nechtějí vážit cestu na služebnu, mají málo času nebo mají třeba i obavy z úředního jednání. Prostřednictvím Pol Pointu se občan může účastnit i soudního řízení - systém je propojený s videokonferencemi ministerstva spravedlnosti.

Pol Pointy představují nový bezobslužný způsob komunikace občana s policií, kdy oznamovatel nemusí čekat na policejním oddělení na příjezd policisty, který třeba zrovna řeší události v terénu, ale může vyřídit svou záležitost okamžitě – pomocí moderní a zabezpečené videokonference. Díky technologiím Cisco Webex, na kterých tato kontaktní místa běží, je tato forma komunikace vysoce spolehlivá a o kvalitu zvukového či vizuálního přenosu se není potřeba obávat.

JAK SYSTÉM POL POINT FUNGUJE

Tato nová alternativa komunikace občana s policií – „Pol Point", asistovaná digitální služba, je založena na již vybudované síti videokonferenčního systému Cisco Webex. Občan může systém Pol Point využít podle svého uvážení, nikoliv však v tísni. Pokud je ohrožen na zdraví a životě sám, nebo někdo jiný, přednostně platí využití tísňové linky 158. Bezpečná kontaktní místa umožňují občanům vytvářet soukromé prostředí k podání oznámení. Mohou jej využít v případě, že se sami stali obětí trestného činu a výslech na policejní služebně by považovali za újmu, nebo chtějí podat oznámení o trestném činu nebo jiném protiprávním jednání, o kterém se dozvěděli. Důvod pro využití kontaktního místa může být pro občana ale i ryze pragmatický, tedy pohodlí a úspora času.

V rámci projektu jsou na území Středočeského kraje zřizována místa s videokonferenčními jednotkami a současně bylo vytvořeno centrální místo – oddělení příjmu trestního oznámení (OPTO), které je dostupné každý den (včetně víkendů a svátků) od 8.00 do 22.00 hodin. První Pol Pointy vznikaly začátkem roku 2020 a jejich síť se postupně rozšiřuje.

Policista může bezodkladně přijmout oznámení a dokumentovat jej. Virtuální způsob komunikace umožňuje přijmout oznámení z jakéhokoliv místa a obratem jej postoupit příslušnému policejnímu orgánu k dalšímu šetření. Občan, který oznámení podává, nemusí nic podepisovat, protože průběh celého výslechu se nahrává a nahrávka se přikládá ke spisu. Policista je zároveň jediný, kdo může autoritativně ověřit totožnost občana na dálku. Díky osobnímu ověření není nutné v lokalitě Pol Pointu řešit ověřování pravosti průkazu totožnosti. Tento způsob zároveň snižuje administrativní zátěž policistů, a naopak zvyšuje jejich operativnost, flexibilitu a ve svém důsledku zrychluje reakce policie na aktuální problém občanů.

PROJEKT NABÍZÍ HNED TŘI ZPŮSOBY KOMUNIKACE

Systém Pol Point je z technického hlediska nadstavbou již zavedené infrastruktury videokonferencí v trestním řízení, která je v praxi středočeských policistů běžně používána. Projekt Pol Point je budován jako soubor tří základních způsobů komunikace podle místa, odkud občan s policistou komunikuje.

Ovládání Pol Pointu je jednoduché a intuitivní, protože vychází z profesionální videokonferenční platformy Cisco Webex.

Prvním způsobem je budování míst, která jsou zřizována jako bezobslužné místnosti, kam může občan vstoupit a bez jakéhokoliv vlastního zásahu začít komunikovat prostřednictvím umístěného videokonferenčního zařízení s policistou, který videokonferenci ovládá z operační místnosti na krajském ředitelství. Tato zabezpečená místa s možností nepřetržitého provozu vznikají jako samostatné místnosti při obvodním oddělení PČR nebo v budovách obecní policie. Terminály umístěné v těchto místnostech jsou napojeny přímo do VPN sítě.

V případě, že se občan dostaví k zabezpečené místnosti, policista mu z centrálního místa po krátké komunikaci prostřednictvím domovního telefonu umožní vstup. To bez elektronického odemknutí na dálku není možné. Po vstupu občana do místnosti se policista z operační místnosti připojí na monitor a s občanem komunikuje videokonferenčně. Občan nemusí nic ovládat a před zahájením úkonu je poučen a upozorněn na pořizování nahrávky. Za oznamovatelem, který je v místnosti, nemůže nikdo jiný vstoupit, naopak on sám z ní může kdykoliv odejít. Výhodou těchto místností je tedy nejen jejich technické vybavení, ale i vytvoření „bezpečné zóny" pro oznamovatele.

Druhým způsobem je budování míst s částečnou obsluhou. Ta jsou zřizována při obecních úřadech, kde základní funkce systému zajišťují pověření pracovníci obecního úřadu. Na úřadech je vytvořena místnost, odkud může občan s policistou nerušeně komunikovat. V případě, že se občan dostaví do místnosti na obecním úřadu, je postup obdobný jako u bezobslužné místnosti, jen s tím rozdílem, že pracovník příslušného obecního úřadu předem ověří totožnost oznamovatele a zprovozní mu videokonferenční zařízení. Provozní doba takového Pol Pointu pak odpovídá úředním hodinám obecního úřadu.

Třetím způsobem je možnost komunikace z místa čistě virtuálního, tedy z vlastního technického zařízení (osobní počítač, notebook, tablet, telefon) občana, který se prostřednictvím tzv. softwarového klienta připojí z veřejné sítě zabezpečeným způsobem do VPN sítě. Tohoto způsobu lze využít i v případech, kdy policisté vyjíždějí na tísňové volání, po příjezdu na místo provedou potřebné úkony a v případě, že je potřeba vyslechnout oznamovatele nebo další osoby, předají instrukce o možnosti spojení prostřednictvím videokonference z osobního počítače. Výhodou tohoto způsobu připojení je neomezený prostor, odkud se může občan připojit, třeba z domova, ze zaměstnání nebo i ze zahraničí. Důležité je samozřejmě patřičné technické vybavení a dostatečná kvalita internetového připojení na straně oznamovatele. Do budoucna lze předpokládat i obdobnou komunikaci občana s dalšími úřady nebo organizacemi, zejména z terminálů umístěných na obecních úřadech.

Kde vznikla myšlenka Pol Pointu?

Vůbec první Pol Point na území České republiky vznikl ve Středočeském kraji v roce 2020, kdy byl díky iniciativě ředitele Krajského ředitelství Policie Středočeského kraje brig. gen. Václava Kučery odstartován pilotní projekt. Nyní jich ve Středočeském kraji funguje již 30, a to ve třech základních modifikacích. „Do současné doby se nám podařilo zprovoznit tři desítky Pol Pointů ve Středočeském kraji, včetně tří mobilních, a jeden v Karlovarském kraji. Dále však chceme kontaktní místa rozšiřovat tak, aby byly dostupné doopravdy pro všechny ze Středočeského kraje. Součástí tohoto systému je i dohoda s tlumočníky, včetně tlumočníků jazyka znakového, čímž jsme schopni vzdáleně poskytnout pomoc bez jakýchkoliv bariér," přiblížil autor projektu a současně ředitel středočeské policie generál Kučera.

Technologie Cisco Webex využitá v Pol Pointech je standardní také při soudních jednáních v USA.

Jaké jsou přednosti Pol Pointu?

Podání oznámení prostřednictvím Pol Pointu má pro oznamovatele své nesporné výhody, a to efektivní a rychlý kontakt s policistou, pohodlí a úsporu času. Mezi další přednosti patří technické vybavení této místnosti umožňující vzdálený kontakt s policistou (což některé oběti vzhledem k charakteristice protiprávního jednání, které na nich bylo spácháno – např. domácí násilí, znásilnění apod., upřednostní před osobní návštěvou policejní služebny) a rovněž vytvoření bezpečného místa pro oznamovatele. Pozitivum můžeme shledat i v podobě nižší administrativní zátěže pro samotné policisty.

CISCO™

5. ROČNÍK KONFERENCE

Snadná navigace

JAK SE NEZTRATIT V ON-LINE SVĚTĚ ÚŘADŮ

MEZINÁRODNÍ KONFERENCE PŘEDSEDNICTVÍ ČR V RADĚ
EVROPSKÉ UNIE VE SPOLUPRÁCI S EVROPSKOU KOMISÍ

22. a 23. listopadu 2022

Kongresové centrum Praha

Dvoudenní odborná konference k digitální transformaci veřejné správy, která nám usnadní orientaci v on-line světě veřejné správy. Snadná navigace pro občany, podnikatele, úředníky a zástupce veřejné správy.

Zajímavé panelové diskuse s hosty, kteří o digitalizaci nejen mluví, ale také ji opravdu dělají.

Odborné prezentace tuzemských i zahraničních řečníků a příklady z jejich praxe.

Co nás čeká, co se daří a co se dalo udělat lépe na příkladech z ČR i ze zahraničí.

Konference bude probíhat v češtině a angličtině s tlumočením do češtiny.

TĚŠIT SE MŮŽETE NA DISKUZE, PREZENTACE, PŘÍKLADY, ZAJÍMAVOSTI Z OBLASTI:

- komunikace s veřejností, propagace digitálních nástrojů, zkušenosti s povinným či dobrovolným využíváním digitálních nástrojů
- digitální identita
- digitální veřejné služby
- digitální vzdělávání
- digitalizace ve zdravotnictví
- digitalizace na lokální úrovni
- interoperabilita a architektura veřejné správy
- open data a další aktuální témata

www.snsu.cz

NAKIT · MINISTERSTVO VNITRA ČESKÉ REPUBLIKY · gov.cz · EU2022.CZ · Evropská komise

eIDAS2.0
Elektronická peněženka na obzoru

Dalším důležitým tématem diskuze v rámci konference v Mikulově bylo nařízení eIDAS2.0. To přináší tzv. evropskou elektronickou peněženku, tedy aplikaci v mobilních zařízeních, která je schopna prokazovat naši elektronickou identitu. Tato peněženka by, kromě samotné identifikace, měla být schopna rovněž nést další doklady (rodný list, řidičský průkaz, různé osobní licence a diplomy) a ty by na naše přání mohly být zpřístupněny, pokud je potřebujeme někde doložit.

Elektronická peněženka by svým zaměřením měla směřovat do širokého komerčního záběru. Dnes totiž elektronickou identitu používáme v drtivé většině pouze pro komunikaci se státem, maximálně bankami, eIDAS2.0 slibuje daleko širší využití. Navíc by měla tzv. e-wallet, jak se elektronická peněženka označuje, být schopna pracovat i offline. To jsou základní prvky, které jsou v tuto chvíli o celém záměru známé. Evropský parlament by měl o návrhu hlasovat na konci října. Od schválení výsledného návrhu bude pravděpodobně limit 12 měsíců pro realizaci v jednotlivých státech. Na podium jsme si pozvali Ivana Bartoše, vicepremiéra pro digitalizaci, Petra Kuchaře, ředitele odboru hlavního architekta MV ČR, Jana Tomíška, právníka Rowan Legal, Tomáše Hebelku, generálního ředitele Státní tiskárny cenin, a Jana Blažka, předsedu představenstva Bank ID.

Ivan Bartoš považuje rozhodnutí o elektronické peněžence za správné. Jak řekl, už covid pas, se kterým jsme se naučili velmi rychle pracovat, ukázal, že potřeba doložení nějakých skutečností jak v kontaktu s domácím e-governmentem, tak zahraniční státní správou či službami napříč Evropou je zcela legitimním požadavkem a přitom „byznysově" pozitivní model. Jednotlivé státy se v tuto chvíli nacházejí v různých fázích implementace svých národních identit, proto logicky přichází otázka směřující na zajištění přesahu směrem za jejich hranice. Nyní v rámci našeho předsednictví se nacházíme v procesu hledání konsensu k tomuto návrhu. Je velice pravděpodobné, že se shodneme na cíli, aby do roku 2030 mělo 80 % občanů zajištěn přístup k elektronickým službám. Není přitom podstatné, zda přístup bude ve výsledku v konkrétním státě zajišťovat stát, soukromý sektor nebo v kombinaci. To je na rozhodnutí jednotlivých vlád. Výsledkem by měl být pozitivní efekt, který budou pociťovat jak poskytovatelé, tak uživatelé.

Petr Kuchař zdůraznil, že jedním z hlavních cílů je skutečně to, aby tím, kdo čerpá služby a výhody z peněženky, byl i soukromý sektor. To je výrazná změna paradigmatu. Současné nařízení (eIDAS1.0) pouští soukromý sektor do role poskytovatelů identitních služeb, ale nikoliv do role klientů. Ta se v tomto smyslu týká jen OVM. Největší změnu přináší eIDAS2.0 právě v tomto posunu směřujícímu ke zvětšení portfolia využití.

Vedle tohoto zaměření je podle Petra Kuchaře další důležitá otázka, která se nyní probírá, zda tato evropská peněženka bude zařízení na úrovni vysoká. Pokud ano, tak to znamená, že musí dojít buď k fyzické identifikaci jejího držitele, tedy že se někam dostaví, ukáže občanku a bude nějak ztotožněn, anebo se tento proces založí na jiném již existujícím prostředku, u něhož už k této identifikaci před tím došlo. Jenže naše banky mají v tuto chvíli prostředky na úrovni střední, čili by to byl drobný problém. Pokud tedy budeme najednou chtít udělat e-wallet na úrovni vysoká, bude nutné určitým způsobem vyřešit tento přechod. Náš opoziční návrh byl umožnit i úroveň střední právě pro snadnost přenosu současných identit. Ale je to politická otázka a zdá se, že tento návrh nám neprojde, protože většina států je pro úroveň záruky vysoká.

Další otázka je, zda skutečně bude implementační lhůta 12, nebo 24 měsíců od schválení legislativy. A další důležité rozhodování tentokráte na národní úrovni, zda kromě národní peněženky připustíme nějaké další soukromoprávní peněženky. Možná budou další, ale nesmí jich být naopak moc, aby to nebylo pro občany příliš zamotané.

Jan Tomíšek uvedl, že právní rámec je paradoxně relativně volný a nabízí hodně způsobů, jak jej naplnit. Novela nařízení eIDAS v podstatě říká, že členský stát buď může wallet vydat, nebo někoho pověřit jeho vydáním, nebo může někomu vydání umožnit. To je podobné jako s elektronickou identitou, jenom tam je povinnost členského státu, aby jednu z těch variant zařídil, ale kterou zvolí, je na něm. Dává to tedy velký prostor, ale i velkou odpovědnost v tom, že nemůžeme čekat na to, co se stane v Evropě. Tam se povede diskuze o otázkách, jestli 12 nebo 24 měsíců, řadě aspektů tohoto typu, které je nutné dořešit, ale základní obrys toho, jak by měla taková peněženka vypadat, je již zřejmý. Je tedy velice důležité, abychom na národní úrovni nezačali přemýšlet, jak to překlopit do české legislativy, ale jak by měl tady u nás v návaznosti na naši architekturu e-governmentu vypadat ten ekosystém. Jde o to, aby se z e-wallet nestal nástroj, jehož realizaci si sice odškrtneme, splníme nařízení, ale bude ho používat minimum uživatelů. Jde o to, aby se z ní stal skutečně nástroj, který 80 % obyvatel přiblíží elektronické služby.

Jan Tomíšek vidí ještě jedno riziko, a to je nařízení o ochraně osobních údajů. Už dnes přibývá služeb, které jsou na úrovni vysoká. Nařízení eIDAS 2.0, jak bylo řečeno, bude pravděpodobně obsahovat úroveň vysoká. Tím začne růst její penetrace a my budeme najednou pod tlakem, protože tady budou některé podstatné služby „jen" na úrovni značná (například e-recept). Jde tedy o to, jestli bychom s takovým postojem obstáli za pět let. To je legislativní riziko, které klade vysoké nároky na správnou implementaci e-wallet. Je přitom zřejmé, že stejně jako bankovní identita nemohla vzniknout bez spolupráce státu a bankovního sektoru, totéž platí pro wallet. Musí to být řešení na průsečíku.

Tomáš Hebelka uvedl, že STC nejen tiskne doklady, ale dělá i digitální projekty, u kterých se skutečně nic netiskne. V diskuzi ale reprezentuje stranu výrobce toho fyzického dokladu. Připomenul, že od roku 2018 se vydávají eOP s čipem a elektronickým certifikátem na úrovni vysoká. O té doby jsme vydali přes 4 mil. eOP. Tedy existuje 4 mil. certifikátů na úrovni vysoká, které ale vůbec nejsou využívány nebo spíš minimálně, protože stát toto neuměl mezi lidi infiltrovat. Naopak v případě Bank ID se to povedlo razantně. Je to jednoduché a uživatelsky příjemné. Je tedy vidět, že cesta spolupráce státu a komerčního sektoru je výrazně úspěšnější. Spousta států (Švédsko, Finsko, ...) už má nějaký takový e-wallet, který sebou nese jednotlivé doklady. Je tu tedy praxe, kdy jde vždy o zapojení státní tiskárny. My máme znalost, know how dokladů – ty doklady se stěhují z fyzického do virtuálního světa, přičemž je nutné zajistit používání obou, proto je důležitá role STC.

Jan Blažek řekl, že se jedná rozhodně o vítanou iniciativu. Hlavní otázka by nyní měla znít, jak chceme nastavit ten ekosystém, aby skutečně fungoval, aby byly firmy motivovány k používání, aby byli klienti i stát, ti všichni, byli motivování k používání. Je samozřejmě nutné se dívat, co e-wallet přináší a jak by měl být vhodně v ekosystému umístěn, aby splňoval vytčené cíle. Tady není podle jeho mínění nutné čekat na rozhodnutí Evropské unie. Měli bychom hledat co největší profit z toho, co e-wallet nabízí s tím, že si nerozbijeme stávající systém. Pro banky se podle jeho slov jedná o stěžejní téma. Byl vydán poziční dokument na úrovni ČBA, kde je řečeno, že banky chtějí se státem nadále v této oblasti spolupracovat a pomoci státu postavit a provozovat systém. Stát však musí proces regulovat majetkově, legislativně a dávat záruky veřejnosti.

ADWnow!

neit·consulting
neit:group

ORACLE | Partner

Poskládejte si s námi **datový sklad bez starostí...**

... a zabavte na chvíli i své děti :)

automation
auditability
all in
agility
autonomous
as a service

ADWnow!
datawarehouse

www.**adwnow**.cz

Směrnice NIS2 a kybernetická bezpečnost ve veřejné správě

Počátek veřejnoprávní regulace kybernetické bezpečnosti v České republice lze datovat od 1. ledna 2015, tedy k datu účinnosti zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Zákon od této doby prošel řadou změn, za tu doposud největší lze považovat novelizaci z roku 2017 vyvolanou přijetím směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii („směrnice NIS"). V současné době lze očekávat změnu srovnatelného, a možná i většího rozsahu v souvislosti s přijetím revize této směrnice, pro kterou je nyní používáno označení „NIS2".[1)]

Předně je nutné poznamenat, že směrnice NIS2 v tuto chvíli nemá schválené finální znění – legislativní proces na úrovni Evropské unie doposud nebyl ukončen a finální znění směrnice nebylo publikováno. K publikaci směrnice NIS2 by mělo dojít na konci roku 2022. Do té doby je možné vycházet z doposud dostupné verze směrnice, která je nyní ve fázi posledních úprav před její publikací. K některým dílčím změnám tak může ještě stran textu směrnice NIS2 dojít a následující text tak čerpá z aktuálních dostupných informací. **Ze současného znění směrnice NIS2 a nastavené transpoziční lhůty pak také plyne, že by se související změny měly promítnout do zákona o kybernetické bezpečnosti v polovině roku 2024.**

NIS2 přináší zcela nový přístup ke stanovení povinných osob, které se jí musí v rámci členských států řídit. Pro srovnání, český zákon o kybernetické bezpečnosti byl a je postaven na dopadovém principu – povinnou osobou se stává jen organizace, která může v případě narušení bezpečnosti svých systémů způsobit společnosti nějakou předem definovanou škodu.[2)] NIS2 tento přístup sice také používá, nicméně až jako doplňkový. **Primárním principem stanovení povinných osob je kombinace poskytování dané služby** (uvedené v přílohách) **a velikosti organizace dle doporučení Komise.[3)]** Obecně tak, z důvodu této změny a rovněž rozšíření počtu odvětví a pod ně spadajících služeb z původních 7 odvětví s 30 službami na momentálně navrhovaných 18 odvětví s 60 službami, bude pod zákon o kybernetické bezpečnosti spadat minimálně patnáctinásobek současného počtu osob. Odhady hovoří nejméně o šesti tisících regulovaných subjektů.

Regulace veřejné správy zůstávala doposud na zvážení samotných členských států a nepatřila mezi povinně regulovaná odvětví, nyní je však v rámci přílohy směrnice NIS2 zařazena a k její regulaci tak bezpochyby dojde. Vzhledem k obsahu se směrnice NIS2 bude bezpodmínečně týkat ústředních orgánů státní správy a regionálních orgánů veřejné správy. S přihlédnutím k tomu, že je žádoucí určitým způsobem zachovávat kontinuitu, lze očekávat, že majoritní část veřejné správy spadající již nyní pod zákon o kybernetické bezpečnosti bude regulována i po transpozici směrnice NIS2. Dále se pak úvahy o budoucí podobě zákona o kybernetické bezpečnosti ubírají směrem k zahrnutí obcí s rozšířenou působností mezi

---

[1)] Současná podoba návrhu směrnice NIS2 je dostupná zde: https://osveta.nukib.cz/pluginfile.php/58363/course/section/1231/NIS2_aktu%C3%A1ln%C3%AD_zn%C4%9Bn%C3%AD.pdf

[2)] Srov. prováděcí právní předpisy sloužící ke stanovení povinných osob podle zákona o kybernetické bezpečnosti – nařízení vlády č. 432/2010 Sb., vyhlášku č. 437/2017 Sb. nebo vyhlášku č. 317/2014 Sb.3)

[3)] Doporučení Komise ze dne 6. května 2003, týkající se definice mikropodniků, malých a středních podniků, dostupné zde: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32003H0361

Empower action with data insights

Discover and exploit critical data insights that drive government transformation and advancement.

SAS® Analytics for state and local government

Using analytics to better serve the public

Data in government is vast. It covers everything from health care to juvenile justice to education and transportation. Accessing a clear, timely picture of the data landscape gives decision makers the unique ability to drive change that improves citizen lives.

Enterprise analytics for government effectiveness

Government organizations use SAS Analytics on an enterprise level for timely, high-quality, reliable and integrated big data assets that drive government transformation. This is done through better decisions, proactive programming and improved efficiencies.

Find the perfect balance of choice and control

With the SAS Platform, you can embrace control and have enough choice to be nimble. Flexibly manage your resources with a variety of SAS and open source analytics tools to get insights from your data. And keep data governance and model management a priority.

Learn more at **www.sas.com/gov**

Questions? Contact us directly at **info@cze.sas.com**.

sas
POWER TO KNOW®

povinné osoby, konkrétně pak v režimu nižších povinností. Objem služeb, které tyto obce zajišťují pro občany, se v souvislosti s nedávnými incidenty ukázal jako rozsáhlý a předznamenal tak potřebu akcentace kybernetické bezpečnosti těchto organizací.

Samotná směrnice NIS2 požaduje roztřídit povinné subjekty do dvou skupin (essential a important) a v rámci této distinkce příslušně určit míru povinností, které budou povinné osoby muset plnit. V současné době je počítáno s tím, že režimy označíme jako režim vyšších povinností (essential) a režim nižších povinností (important).

Tato distinkce se tak musí projevit zejména v rámci bezpečnostních opatření, kde je v současné době počítáno s tím, **že pro režim vyšších povinností bude aplikována novelizovaná verze vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, pro režim nižších povinností pak vzniká vyhláška nová, která povinnosti stanovuje na základnější úrovni**, tedy je spíše blíže např. minimálnímu bezpečnostnímu standardu, který Národní úřad pro kybernetickou a informační bezpečnost („NÚKIB") v minulosti vydal.[4)]

Vzhledem k markantnímu nárůstu počtu povinných subjektů bude muset dojít i k dalším úpravám v rámci procesu **identifikace povinných osob (nově bude primárně ovládána principem sebeidentifikace dle kritérií daných příslušným prováděcím předpisem) a v rámci další komunikace s NÚKIB (elektronizace procesu)**. Připravuje se tak jednotný informační systém, který by měl zaštítit jak registraci povinných osob, tak následnou komunikaci s NÚKIB, např. ve formě hlášení incidentů.

Návrh směrnice klade také velký důraz na roli vrcholového vedení organizace. To by se mělo mnohem více zapojovat do řešení problematiky kybernetické bezpečnosti, protože jak se v praxi stále ještě ukazuje, vedení organizací považuje kybernetickou bezpečnost za dílčí problém, vhodný k řešení nejlépe na úrovni vedoucího IT oddělení. Z tohoto domnění je může přinejhorším vyvést jedno z nových ustanovení, které v případě povinných osob v tzv. režimu vyšších povinností zavádí jako krajní možnost uložit i dočasný zákaz výkonu manažerských funkcí příslušné fyzické osobě. Dalším možným postihem je i pozastavení licence pro poskytování dané služby pro celou organizaci.

Poslední velkou změnou je změna přístupu k ukládání pokut za porušení zákona.
Návrh směrnice se ve věci pokut inspiroval v Obecném nařízení o ochraně osobních údajů (tj. GDPR). Pokuty jsou tak nově stanoveny na 10 000 000 EUR nebo 2 % celkového celosvětového ročního obratu organizace v případě režimu vyšších povinností, resp. na 7 000 000 EUR a 1,4 % v případě režimu nižších povinností.

Na závěr lze pro bližší informace odkázat na web provozovaný NÚKIB (nis2.nukib.cz), který má za cíl informovat o směrnici NIS2 blíže a k výše uvedeným, ale i dalším tématům zde naleznete další užitečné informace[5)].

Daniela Procházková
vedoucí oddělení
Oddělení regulace veřejného sektoru
Národní úřad pro kybernetickou
a informační bezpečnost

[4)] Dostupné zde: https://www.nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf
[5)] Dostupné zde: https://osveta.nukib.cz/course/view.php?id=145https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32003H0361

HPE GreenLake

Modernize with the cloud that comes to you

Should you move all your apps and data to the cloud? You can choose not to choose with HPE GreenLake—the platform that brings the cloud to you.

Visit **GreenLake.HPE.com**

HPE GREENLAKE | EDGE-TO-CLOUD PLATFORM

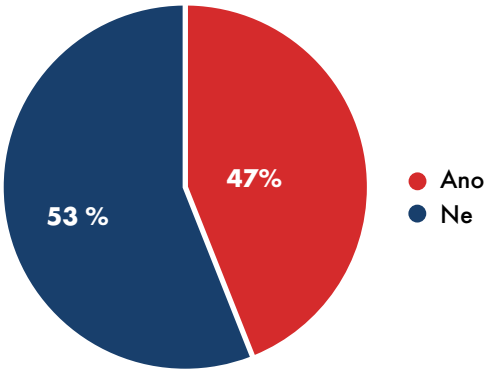
Češi se hlásí o elektronickou identitu. Neumí ovšem digitálních služeb využívat naplno

Na tradiční konferenci Egovernment, která se konala začátkem září v Mikulově, zazněly zajímavé informace o aktuálním využívání digitálních služeb státu. Ve stejném období probíhal průzkum společnosti Gordic* o připravenosti obyvatel na digitalizaci veřejné správy. Závěry prezentací a průzkumu ukazují, že stát digitalizovat chce, snaží se občanovi umožnit komunikovat elektronicky, akceptuje další identifikační prostředky i od soukromých poskytovatelů a tak dále. Na druhou stranu jsou občané málo informováni, proces se často zdá velmi náročný nebo ne příliš efektivní. Podívejme se na některá čísla.

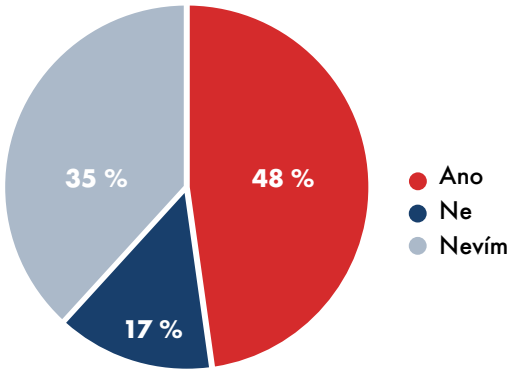
Jak na konferenci uvedl Petr Kuchař z Ministerstva vnitra, alespoň jedním identitním prostředkem, tedy například datovou schránkou nebo bankovní identitou, už disponuje pět a půl milionů občanů. V praxi ho zatím použilo 1,8 milionu. K nárůstu uživatelů digitálních služeb přispěla za poslední rok právě bankovní identita. Nejvíce aktivní jsou v této oblasti klienti České spořitelny. Téměř půl milionu z nich využilo svou bankovní identitu v kontaktu se státem. Následují pak klienti ČSOB (více než 300 tisíc) a Komerční banky (téměř 240 tisíc).

Průzkum společnosti Gordic ukázal, že navzdory počtu identitních prostředků Češi digitalizaci veřejnosprávních úkonů ve větším měřítku nevyužívají. Neznamená to ale, že by o elektronickou komunikaci s úřady nestáli. Většina lidí (55 %) si totiž myslí, že jim stát nedává dostatečné možnosti na to, aby své úkony mohli vyřizovat digitálně. Problémem ale může být špatná forma propagace nebo dostupnost informací o digitálních službách. Více než polovina dotazovaných (53 %) potvrdila, že neví, kde je mohou hledat. O nedostatečné informovanosti svědčí i otázka o možnosti hradit poplatky a řešit životní situace ve své obci online. Třetina lidí (35 %) vůbec neví, jestli tuto možnost v místě bydliště mají.

Víte, kde informace o dostupných digitálních službách hledat?



Umožňuje vám vaše město/obec vyřídit životní situace a hradit poplatky elektronicky?



**Sběr dat byl realizován prostřednictvím aplikace Instant Research agentury Ipsos v srpnu 2022 za pomoci dotazování reprezentativního vzorku 800 Čechů a Češek ve věku 18 až 65 let.*

Z průzkumu společnosti Gordic

Státní Portál občana, kam se můžete přes svou digitální identitu přihlásit, umožňuje pohybovat se v portálech úřadů, jako finanční správa, e-recept nebo očkovací portál – i přesto ho ale navštívila méně než polovina dotazovaných (46 %). Z cca 400 služeb, které Portál nabízí či zprostředkovává, byl v roce 2021 nejžádanější výpis z rejstříku trestů pro fyzické osoby (48 236 žádostí). Výrazný zájem je dále např. o výpis z živnostenského rejstříku (18 642 elektronických výpisů), výpis z bodového hodnocení řidiče (16 000 výpisů) nebo o elektronickou žádost o nový řidičský průkaz (16 000 žádostí od spuštění služby 1. června 2021). Data také ukazují, že datovou schránku, která umožňuje elektronickou komunikaci mezi státem a občanem bez nutnosti chození na úřady, vlastní jen menšina dotazovaných (22 %). To se však s příchodem dalšího roku změní, jelikož Ministerstvo vnitra začne datové schránky zakládat automaticky při využití bankovní identity.

Na výše jmenované konferenci mj. zaznělo, že ti lidé, kteří svou elektronickou identitu již využili, ji nejčastěji potřebovali pro přihlášení do Portálu občana, přístup k očkovacímu portálu ÚZIS, při sčítání lidu 2021 nebo v souvislosti s covidovými programy v době pandemie. V letošním roce se však jednoznačně největšímu zájmu těší aplikace MPSV Jenda, jejíž prostřednictvím lze žádat o jednorázový příspěvek 5 000 Kč na dítě. Díky ní bylo evidováno přes 1 mil. nových žádostí o digitální identitu.

Aktivní v poskytování služeb však není pouze stát, ale i města a obce. Ty prostřednictvím svých lokálních portálů občanů nabízejí možnost vyřídit běžné záležitosti, jako zaplatit poplatek za parkovací kartu či za odpady nebo přihlásit psa. „V těch službách je ještě velký potenciál, zdaleka ne všechna města disponující portálem občana, v němž by provozovala všechny nabízené služby. Portály jsou propojené s platební bránou, není tak problém se z domova přihlásit a třeba zaplatit pokutu za špatné parkování platební kartou," říká Vít Kasal ze společnosti Gordic.

Nárůst uživatelů svého portálu občana zaznamenali například ve Znojmě nebo Prostějově, a to v řádu stovek nových přihlášení. Nejčastějším úkonem, pro který prostějovští občané portál využívají, je žádost o dotaci. Právě pro řešení grantů a dotací se nabízí využití funkcionality z Portálu občana GORDIC, tzv. zastoupení právnických osob. Za právnickou osobu vždy musí jednat k tomu určená či zmocněná fyzická osoba. Po založení právnické osoby v portálu získá při dalším přihlášení možnost zvolit, zda chce jednat za sebe či za přiřazenou organizaci.

Průzkum také odkryl některé nedostatky při poskytování digitálních služeb. Například portály při velkém zatížení často nefungují. Mělo by se tak dbát o zvýšení kapacitních nároků na provoz informačních systémů a technologickou inovaci. Další častou výtkou byla nepropojenost portálových řešení. Občan i při digitálním vyřizování musí stále dokola předkládat formuláře, žádosti a jiné informace, které již jednou dodal. Nedostatečná je stále i propagace digitálních služeb. Například není výjimkou, že město svůj portál občana schovává někde hluboko ve struktuře webu. Přitom by to mělo být naopak, občan by měl hned na první pohled vidět, kde se může přihlásit a co vše může digitálně vyřídit.

GORDIC

Citrix poskytuje „ZERO TRUST NETWORK ACCESS“ Bezpečný přístup uživatelů k aplikacím organizace

Bezpečnost informačních technologií získává potřebnou pozornost ve všech sférách společenského života, pro veřejnou správu je v souvislosti s postupující digitalizací a zaváděním eGovernementu specifická v druhu zpracovávaných informací a případných následcích při útoku a výsledném dopadu na společnost. Nedostatek zdrojů spolu s mnohdy již nemoderními koncepty informační bezpečnosti významně ztěžují realizaci řešení, která poskytnou potřebnou ochranu a budou nákladově přijatelná.

Kombinace mnohdy nedostatečné údržby, auditů informačních technologií spolu s konceptem perimetrové ochrany (vnější/vnitřní síť) vytváří prostředí s obtížně řešitelným vzdáleným přístupem zaměstnanců i dodavatelů při zachování potřebné bezpečnosti. Útočníci mají pro průnik do takové organizace bezpočet nástrojů, průnik do samotné sítě je první metou. Následné aktivity jako např. zvýšení oprávnění, detekce síťového zabezpečení a jeho slabin, detekce užívaného SW a případných dalších zranitelností jsou pak další prostor pro bezpečnostní narušitele.

Typickým představitelem tzv. perimetrové ochrany je nejběžněji používaná technologie VPN. Určitě ve své době přinesla uživatelům nové možnosti a způsob, jak rozšířit zabezpečený perimetr i na vzdálené uživatele. Praxe ukazuje, že má svoje limity. Co *je zabezpečené nemusí být ještě bezpečné.*

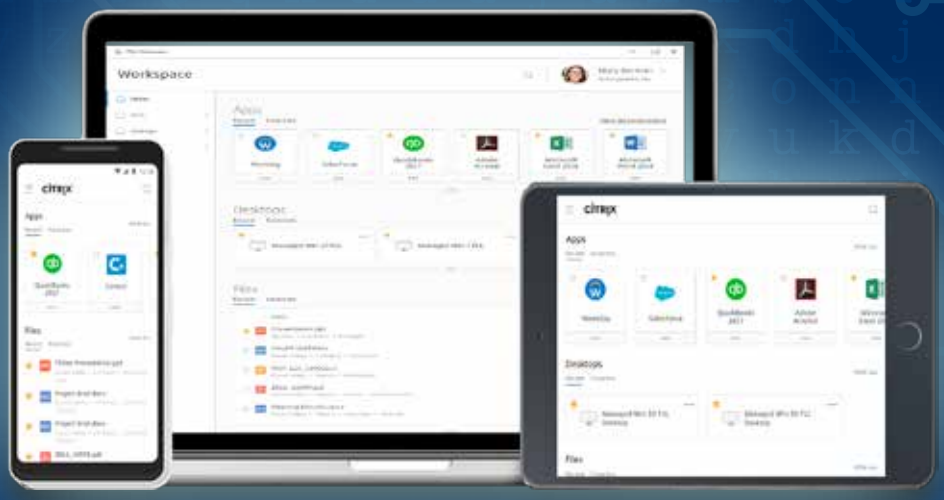
V současnosti se pro přístup uživatelů k aplikacím organizace používá modernější přístup zvaný „ZERO TRUST“. V čem spočívá a jak se liší od VPN si ukážeme na jednoduchém analogickém příkladě, který si jistě každý dovede představit i bez hlubokých technických znalostí. Pro pochopení změn, které se dějí v bezpečnostních přístupech a na ně návazných technologií si zkusme vytvořit analogické příklady vzdáleného přístupu s návštěvním řádem pro budovu/sídlo organizace.

Hosta-dodavatele ze společnosti Supply, vstupujícího do budovy organizace označeným vchodem pro dodavatele, uvítá vrátný/bezpečnostní služba a zjišťuje důvod návštěvy a identitu hosta. Host prokáže totožnost kartou vydanou organizací a jako důvod návštěvy uvede smluvené jednání s vedoucím odboru pro dodavatele (typický příklad uživatele připojeného po VPN, tedy uživatele, majícího oprávnění vstupu).

1. *Vrátný zaznamená detaily do knihy dodavatelů, vysvětlí cestu ke kanceláři vedoucího údržby a dále se o hosta nezajímá. Zvědavý host prochází budovou, vidí mnoho různých dveří a zkouší je otevírat - některé jsou zamčené, ale ne všechny. Do odemčených dveří host vždy jen nahlédne, dokud ho v jedné z přístupných místností nezaujme složka s popisem „Návrh rozpočtu 2023“. Duplikačním nástrojem, který má běžně u sebe, vytvoří kopii složky, a pokračuje do kanceláře vedoucího.*

Tato analogie VPN přístupu bez dalších bezpečnostních opatření ukazuje, že jednoduché ověření identity a deklarovaný/obvyklý důvod vstupu hosta do sítě není bezpečné.

2. *Vrátný ověří v knize dodavatelů, zda je jednání hlášeno, vysvětlí cestu ke kanceláři vedoucího údržby a hostovi udělí oprávnění, která mu dovolí průchod několika zamčenými dveřmi k cílové kanceláři. Na dalších dveřích, které cestou míjí, vidí elektronické zámky a otevírat je raději nezkouší, viditelný sledovací systém brání jeho zvědavosti. V jedné z nepřístupných jednacích místností však přes prosklené dveře zahlédne na hustě popsané nástěnné tabuli nadpis „ Analýza služeb dodavatele Supply“ a o kus níže výrazně podtržené poznámky „finální platbu za dodávku neprovádět, právní oddělení dokončuje přípravu a podklady“. Jedním ze svých nástrojů vyfotí celý obsah tabule včetně dalších detailů a dále pokračuje do kanceláře vedoucího. Po odchodu hosta si vrátný při kontrole časového záznamu pomyslí: „Ještě nikdo nešel na údržbu tak dlouho“.*



VPN přístup do segmentové podnikové sítě doplněný NAC bezpečnostním řešením a monitoringem také neobstojí – hosté si stále mohou donést vlastní nástroje a s jejich pomocí najít a získat citlivý obsah či neoprávněný přístup. Výhoda je na straně útočníka, organizace a její bezpečnostní správci musí zajistit funkčnost a aktuálnost kompletního systému, útočníkovi stačí čekat na chybu.

3. *Vrátný ověří v knize dodavatelů, zda je jednání hlášeno, hosta požádá, aby nechal veškeré své vybavení mimo vnitřní prostory organizace a dovede ho ke dveřím, za kterými je jen prázdná chodba, končící v žádané kanceláři. Z perspektivy hosta tu není nic jiného, než schválený cíl, bez svých nástrojů neumí tento tunel prohlédnout.*

Přístup na aplikační úrovni se od síťového – VPN zásadně liší možnostmi, kterými případný útočník disponuje, čím méně, tím lépe. I v případě získání identity vidí útočník pouze aplikační relaci, což významně ztěžuje další postup. A to je analogie „ZERO-TRUST" přístupu – uživatel dostane přístup pouze ke konkrétním aplikacím, může používat pouze omezené nástroje (externí disky, paměti, USB vstupy,...), navíc je po celou dobu monitorováno, co dělá. Pokud jeho činnost vybočuje z očekávaného normálu, systém se začne chránit.

Zero Trust Network Access, neboli přístup k síti s nulovou důvěrou, řeší bezpečnost koncepčně a kontextuálně šifrování pro vnitřní i vnější komunikaci, trvalá validace přístupových oprávnění a identit, jasné vymezení oprávněných nástrojů a SW komponent pro daný typ úlohy a přístupu.

Problémem je realizovatelnost takové změny při zachování provozu organizace. Řešení Citrix nabízí řešení pro dosavadní (legacy) aplikace, interní webové i moderní SaaS aplikace, rychlé nasazení do stávající infrastruktury, kompatibilitu a integraci s dalšími bezpečnostními prvky, a v neposlední řadě uživatelskou přívětivost pro koncového uživatele.

Nasazení Citrix pro bezpečný vzdálený přístup k aplikacím a datům zakryje podkladové technologie a systémy a umožní jejich postupnou modernizaci, nabídne klíčové funkce jako více faktorovou autentizaci, podrobnou auditní stopu, ověření koncových zařízení mimo správu organizace (BYOD, počítač třetí strany). Díky „ZERO-TRUST" platformě Citrix je organizace schopna vytvořit zcela moderní přístup k zabezpečení svých systémů, který je schopen reflektovat současné hrozby a dále se rozvíjet. A přitom není nutno vše vyměnit, mnoho již používaných technologií lze využívat dál.

https://www.citrix.com/solutionszero-trust-network-access/

Roman Kapitán
Market Development Engineer,, Citrix

citrix®

Dlouhodobé uchovávání elektronických podpisů/pečetí – nová služba I.CA LTA

Společnost První certifikační autorita, a.s., (dále též „I.CA“) nabízí v kombinaci s klientským nebo cloudovým prostředím technické řešení v podobě služby I.CA Long Term Archival (dále jen „LTA“ nebo „služba“), která zajistí dlouhodobé a trvalé uchování elektronických dokumentů obsahujících elektronické podpisy/pečetě.

Vzhledem k tomu, že elektronické certifikáty či kvalifikovaná elektronická časová razítka (dále též „TSA“), které vytvářejí elektronické podpisy/pečetě, respektive které určují datum vzniku elektronických podpisů/pečetí nebo elektronických dokumentů, mají omezenou platnost (u certifikátů obvykle jeden rok, u TSA pět až šest let), je dle povahy elektronického dokumentu nutné zajistit, aby vytvořené elektronické podpisy/pečetě byly i nadále v plnohodnotném a ověřitelném stavu i po expiraci těchto elektronických podpisových/pečetících certifikátů nebo TSA.

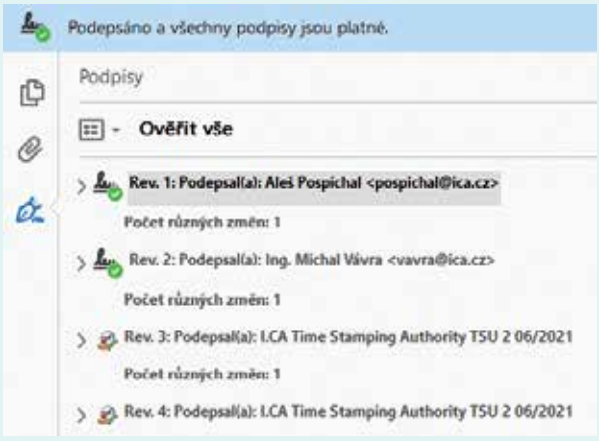
Hlavní podstatou služby LTA je tak postupné ošetřování elektronického dokumentu s elektronickými podpisy/pečetěmi, aby nedošlo k přerušení jejich časové kontinuity. Tím bude zajištěno, že elektronické podpisy/pečetě budou i v budoucnu nadále a jednoduše ověřitelné v běžně dostupných produktech (např. pro formát PDF v produktech Adobe).

V rámci ošetření elektronického dokumentu provede služba LTA nejprve vlastní tzv. LTA analýzu, ve které se definují potřebná validační data (CRL, OCSP, TSA atd.), která jsou nutná pro validaci elektronických podpisů/pečetí. Uvedená validační data jsou následně vložena do elektronického dokumentu k jednotlivým elektronickým podpisům/pečetím a stávají se tak součástí samotného elektronického dokumentu, který si je uchovává ve své vnitřní struktuře. Pro následné ověření elektronických podpisů/pečetí tak již nejsou nutná žádná jiná externí metadata nebo specializované SW, které by musely validitu elektronických podpisů/pečetí následně prokazovat, což je hlavní rozdíl a výhoda oproti tradičním archivům.

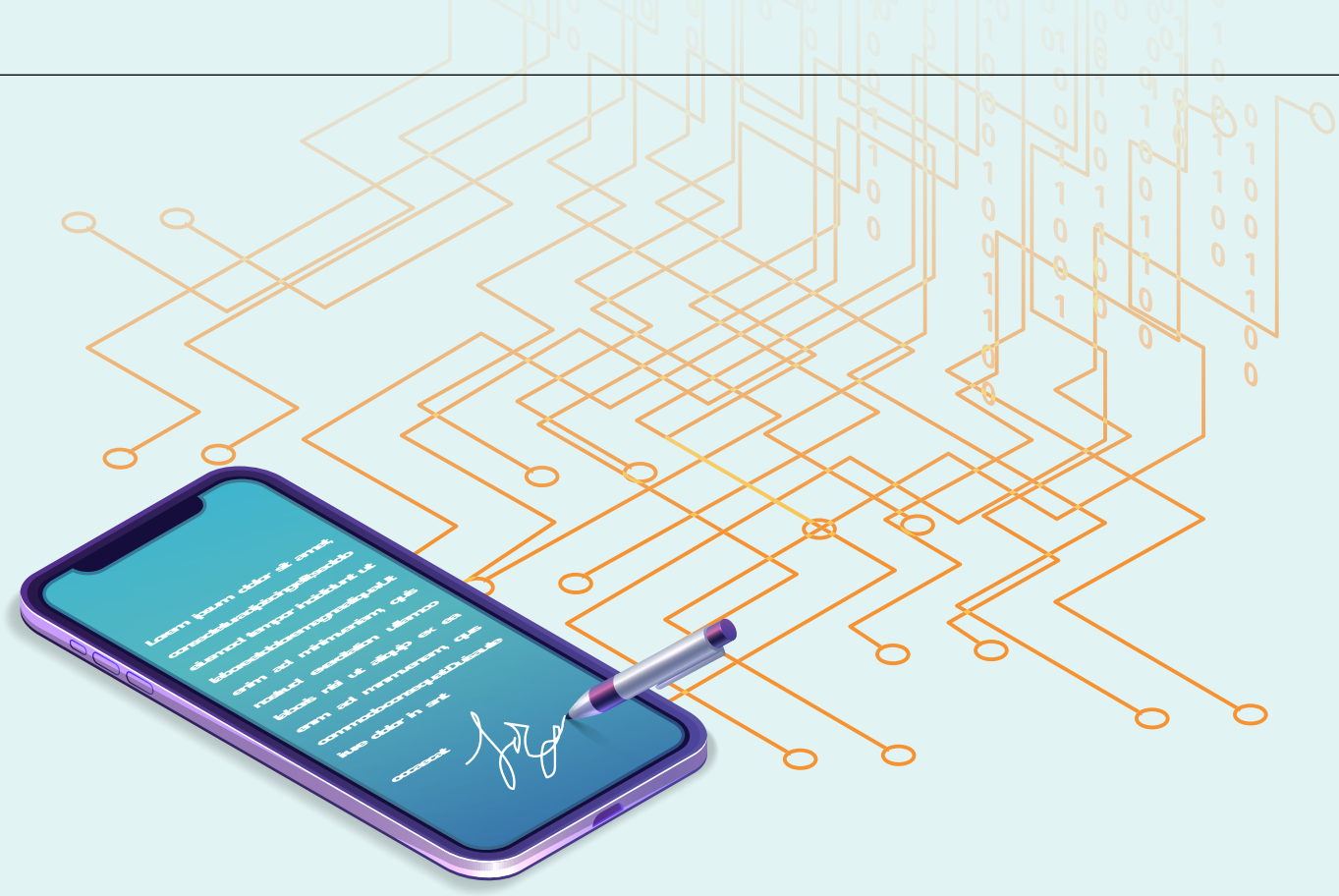
Cílovými archivními formáty elektronických podpisů/pečetí, které jsou službou LTA v jednotlivých typech elektronických dokumentů postupně tvořeny, jsou:

- **PAdES B-LTA** (pro elektronické dokumenty typu PDF);
- **CAdES B-LTA** (pro ostatní elektronické dokumenty);
- **XAdES B-LTA** (pro elektronické dokumenty typu XML).

Uvedené archivní formáty elektronických podpisů/pečetí podle příslušných norem zajistí potřebnou ověřitelnost v čase až do doby skartační lhůty daného elektronického dokumentu. Nejlépe interpretovatelným a z laického hlediska ověřitelným elektronickým formátem je archivní elektronický podpis/pečeť v PDF dokumentech, který v případě jeho vytvoření vypadá dle obr. níže.



Archivní elektronický podpis/pečeť je postupně službou LTA složen. Jeho konstrukce by měla být řešena již systémově, protože se nejedná o jednoduchou záležitost. Archivní formát elektronického podpisu/pečetě je doporučeno vytvářet do jednoho roku od vzniku elektronického



dokumentu nebo tak, jak budou postupně a v průběhu let jednotlivé certifikáty nebo TSA expirovat. Proto analýza LTA na vstupu, a i později opakovaně definuje i interval s hodnotami „od" „do", kdy zejména hodnota „do" určuje nejpozději možný termín pro následné ošetření elektronického dokumentu tak, aby některý z jeho elektronických podpisů/pečetí neexpiroval. Analýza LTA dále také definuje, co se v rámci daného ošetření s elektronickým dokumentem má stát, např. vložit nové TSA nebo další validační data apod.

Ve výsledku archivní formát elektronického podpisu/pečetě obsahuje nebo je postupně složen následovně:

- **PAdES B-B** (typ podpisu obsahuje podpisový nebo pečetící certifikát);
- **PAdES B-T** (typ podpisu obsahuje podpisový nebo pečetící certifikát s TSA);
- **PAdES B-LT** (typ podpisu obsahuje podpisový nebo pečetící certifikát s TSA a validačními daty);
- **PAdES B-LTA** (typ podpisu obsahuje podpisový nebo pečetící certifikát s TSA, validačními daty a následným TSA).

V rámci implementace služby LTA je případně možné si vybrat i typ daného úložiště pro elektronické dokumenty. Službu je možné napojit na klasická DMS, která jsou provozována v klientském prostředí, a nebo je možné ji napojit i na cloudová řešení, kde klientské prostředí provozuje I.CA formou virtuálních serverů.

Z hlediska cenové politiky nejsou na službu LTA kladeny žádné investiční prvotní náklady. Komponentu LTA nebo zprovoznění služby LTA pro klienty zajišťuje I.CA plně zdarma. Následně je po roce hrazen pouze roční support a update. V rámci uchovávání jsou pak standardně hrazeny jen odběry za doplňkové služby, jako je služba odběru TSA a kvalifikovaná služba ověřování elektronického podpisu/pečetě (I.CA QVerifyTL), která realizuje právě analýzy LTA. Uvedené doplňkové služby jsou pak fakturovány dle standardních množstevních ceníků, které již mohou někteří klienti mít s I.CA předem zasmluvněny a u kterých se zvýší pouze jejich odběr. Díky službě LTA se tak uchování jednoho elektronického dokumentu na průměrných deset let s potřebnými důvěryhodnými a zákonnými požadavky může stát pouze korunovou záležitostí.

Ing. Michal Vávra,
manažer klíčových zákazníků,
První certifikační autorita, a.s.,
www.ica.cz

Modelováním agend k vyšší kvalitě údajů VS

Programové prohlášení vlády ČR se poměrně výrazně věnuje problematice e-governmentu a digitalizaci veřejné správy a slibuje v této oblasti významné posuny vpřed. Důležitým prvkem e-governmentu jsou údaje (data) spravované veřejnou správou a jsou jim také explicitně věnovány některé body v prohlášení vlády, jako například:

- ***důsledně budeme vymáhat, aby mezi úřady obíhala data, nikoli občan. Pokud občan státu data jednou poskytne, už je po něm stát nesmí znovu vyžadovat;***
- ***zrychlíme proces otevírání dat (open data) a aktualizace otevřených dat na všech úřadech veřejné správy;***
- ***otevřeme data komerčnímu i neziskovému sektoru a přizveme je, aby se tak podílely na rychlejším rozvoji digitálních služeb veřejné správy a privátního sektoru.***

Problematice dat a údajů veřejné správy je věnován následující text.

Legislativa definuje a vymezuje agendy jako právní rámce pro fungování orgánů veřejné moci v dané oblasti, definuje související procesy a činnosti spojené s jejich výkonem a vymezuje rozsah evidovaných, spravovaných a využívaných údajů pro jejich výkon. Každý konkrétní zákon legislativně vymezuje konkrétní agendu veřejné správy, určuje její konkrétní prováděné činnosti (procesy) a vymezuje nezbytné údaje pro její provádění. Správnost a přesnost každé prováděné agendy je závislá na přesnosti její definice v zákoně. Z pohledu definovaných činností pro výkon agendy se nejedná o zásadní problém, zcela odlišná situace je ale v oblasti údajů, jejich názvů a jejich významů. Údaje spravované v agendě jsou odvozeny od pojmů, jejichž významy jsou s větší či menší přesností definovány souvisejícím zákonem. Celá situace je ale komplikovaná faktem, že pojmy (respektive jejich názvy) jsou sdíleny napříč veškerou legislativou (odlišnými doménami), a tak není výjimkou, že jejich konzistence z pohledu věcného významu bývá nedostatečná.

Z těchto důvodů existují pro tvorbu legislativy doporučené zásady (např. „Metodická pomůcka pro přípravu návrhů právních předpisů" vydaná odborem vládní legislativy Úřadu vlády v roce 2006), avšak k jejich nedodržování dochází poměrně často.

Pro ukázku výběr několika zásad souvisejících s pojmy, a tedy návazně i s odpovídajícími údaji agend:

- pojem je nutné vymezit srozumitelně a jednoznačně a vyhnout se současně definici nevhodné až směšné;
- v rámci určité části právního předpisu, např. dílu, nelze upravovat nový pojem pouze pro účely této části;
- je nežádoucí, aby pojem, kterému je obecně přisuzován určitý obsah, byl pro účely různých zákonů vymezen různě (zásada **stálosti pojmosloví**).

Příklad nejednoznačně definovaného pojmu v legislativě (nedodržení zásady stálosti pojmosloví) – pojem „budova".

- V zákoně č. 256/2013 Sb., o katastru nemovitostí je definována jako *„nadzemní stavba spojená se zemí pevným základem, která je prostorově soustředěna a navenek převážně uzavřena obvodovými stěnami a střešní konstrukcí"*.
- V zákoně č. 406/2000 Sb., o hospodaření energií je definována jako *„nadzemní stavba a její podzemní části, prostorově soustředěná a navenek převážně uzavřená obvodovými stěnami a střešní konstrukcí, v níž se používá energie k úpravě vnitřního prostředí za účelem vytápění nebo chlazení"*.

Význam budovy se v kontextu obou zákonů liší a skutečný a přesný význam pojmů je dán až jejich celým **slovně vyjádřeným kontextem**. Název samotného pojmu je nejednoznačný. V rámci jednoho zákona (jedné agendy) to nemusí být problém, avšak veřejná správa je tvořena množstvím agend, které pojmy (a údaje) navzájem sdílejí a využívají je při jejich výkonu.

Podobných nejednoznačně definovaných pojmů existuje celá řada a očekávat rychlou nápravu těchto nedostatků v legislativě není příliš reálné.

Potřeba jednoznačnosti významu pojmů (údajů) ve veřejné správě se zvyšuje s úsilím při budování e-governmentu. Příkladem může být aktuální znění § 5 zákona č. 111/2009 Sb., o základních registrech. Vedle stávající povinnosti veřejné správy využívat referenční údaje ze základních registrů jako závazné, zavádí zákon tuto povinnost také pro využívání sdílených údajů z agendových informačních systémů napříč agendami veřejné správy. Pro sdílení údajů agendových informačních systémů je určen Propojený datový fond (PPDF) a nově také Veřejný datový fond (VDF), který je vytvářen na principu otevřených dat. Otevřená data jsou určena k obecnému využití, a explicitně definovaný jednoznačný význam jejich jednotlivých publikovaných údajů je proto nezbytný. Efektivním vyjádřením významu jednotlivých údajů je zachycení jejich kontextu v datových specifikacích, například formou konceptuálních modelů.

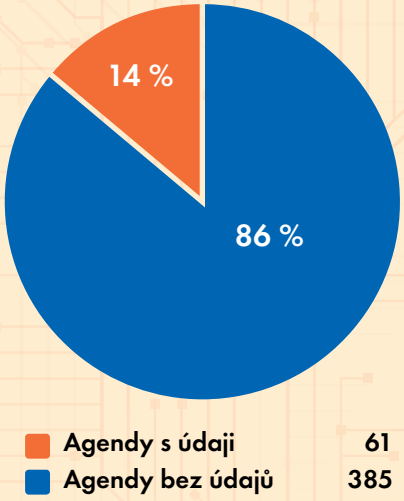
Veřejná správa je z informatického pohledu značně distribuované heterogenní prostředí vyskytující se ve významově rozličných oblastech (doménách), které sdílení a výměnu informací komplikuje. Informační architektura veřejné správy proto řeší složité sdílení údajů centrálním místem, které má za úkol evidovat a spravovat informace o všech subjektech práva (v agendě vystupují v agendových rolích – kontextech) a objektech práva (jsou předmětem práv nebo povinností subjektů práva), jejich údajích (atributech), datových strukturách a souvisejících legislativních ustanoveních. Na základě evidovaných informací o údajích VS následně umožňuje a zprostředkovává sdílení a přístup k údajům napříč všemi agendami. K tomuto účelu je určen jeden ze základních registrů – registr práv a povinností (RPP), který by měl na základě § 51 (6) zákona č. 111/2009 Sb. obsahovat informace o každé agendě veřejné správy, o údajích všech subjektů a objektů práva spravovaných každou agendou, a také o jejich atributech.

K zajištění správné funkcionality sdílení a přístupu k údajům VS je nezbytné, aby informace evidované o nich v RPP byly úplné, významově správně popsané a aby v RPP byly evidovány všechny údaje všech agend.

Reálný stav informací vedených v RPP (srpen 2022) je ale následující:

- registrováno 446 agend 30 ohlašovateli;
- pouze u 61 agend jsou uvedeny nějaké údaje (zahrnuty i agendy pouze s jedním údajem) dle § 51 (6) zákona č. 111/2009 Sb., což představuje pouze 14 % všech ohlášených agend;
- evidováno celkem 214 subjektů a objektů práva s 1637 evidovanými atributy (údaji).

Reálný stav informací vedených v RPP



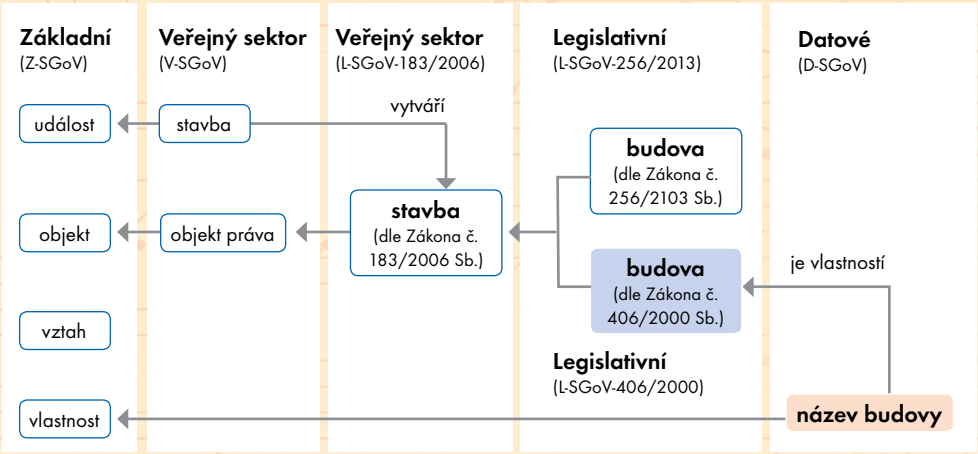
Základní nedostatky a chyby při registraci agend:

- nejsou identifikovány a evidovány všechny subjekty a objekty práva (entity) v agendách dle znění příslušné legislativy;
- častá špatná identifikace entit (nejsou uváděny entity předmětné domény, ale pojmy, které nejsou subjektem ani objektem práva, jako „evidence“, „registr“, různé činnosti apod.);
- schází detailní výčet údajů entit (86 % agend nemá uvedeny žádné údaje).

Stávající stav evidence údajů v RPP je zcela neuspokojivý a neposkytuje dostatečný základ pro sdílení údajů agend dle § 5 zákona č. 111/2009 Sb., o základních registrech. Světlou výjimku představují pouze základní registry a jejich sdílené údaje.

Neúplnosti registrace agend a nejednoznačnostem v definicích pojmů je možné účinným způsobem předcházet sémantickým modelováním legislativy a agend. Pro zachycení významu pojmů v kontextu daného dokumentu nebo domény je využíván „Sémantický slovník pojmů". Ten sdružuje slovníky na různých úrovních, od základního slovníku (Z-SGov – obsahuje především pojmy pro popis ostatních slovníků) přes slovník veřejné správy (V-SGov), který obsahuje pojmy používané napříč veřejnou správou, až po slovníky popisující konkrétní agendy, datové sady a dokumenty.

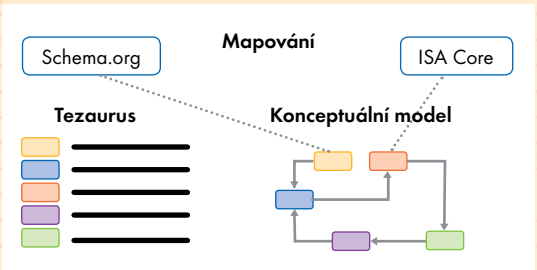
Sémantický slovník pojmů



Každý jednotlivý slovník je tvořen:

- tezaurem (glosářem), který definuje důležité pojmy v dané oblasti zájmu, např. pojmy zavedené nějakým zákonem nebo pojmy používané v nějaké agendě;
- konceptuálním modelem – znalostním grafem, který pojmy z tezauru vzájemně propojuje pomocí významových (sémantických) souvislostí.

Sémantický slovník



Sémantický slovník pojmů veřejné správy (SGoV) se tak stává prostředkem pro postupnou harmonizaci významu (sémantiky) dat vedených v informačních systémech veřejné správy (ISVS). Lze ho chápat jako katalog pojmosloví používaného v rámci veřejné správy, zahrnující pojmy, jejich definice, vazby pojmů na legislativu, vzájemné významové vazby pojmů mezi sebou i významové vazby pojmů na standardní veřejné slovníky používané v zahraničí (především z iniciativy EU, např. ISA Core Vocabularies).

Významová vazba označuje souvislost mezi pojmy, která má určitý konkrétní definovaný význam.
Publikovanou ukázku sémantického slovníku pojmů veřejné správy lze získat prostřednictvím odkazu https://slovnik.gov.cz/.

Dále uvedený obrázek zachycuje zjednodušený rámec tvorby i využití sémantického slovníku.
Proces tvorby sémantického slovníku se skládá z doporučených kroků, které jsou znázorněny na obrázku odstíny žluté. Odstíny zelené zobrazují návazné části procesu, které využívají výsledky konceptuálního modelování například pro tvorbu datových schémat, nebo formulářů určených pro zadávání a sběr dat.

Samotnou tvorbu sémantického slovníku lze tedy popsat několika následujícími kroky:

1. doménový odborník (znalec věcné problematiky) shromáždí dokumenty, které obsahují relevantní terminologii (např. legislativu);
2. sestaví a publikuje pojmový glosář (tesaurus);
3. datový architekt sestaví konceptuální model;
4. publikuje sémantický slovník k obecnému využití.

Váš švýcarský nůž v oblasti doručování aplikací, aplikační bezpečnosti a zabezpečeného přístupu k aplikacím

Load Balancing


L3 a L7 DDOS ochrana


Bezpečný přístup k aplikacím


Global Load Balancing


Firewall


Anti-fraud & anti-bot ochrana


Měření výkonnosti aplikací


SSL dekrypce a orchestrace


Web/Aplikační server


Web/Aplikační Firewall


Enkrypce uživatelských jmen


API Gateway


K8s Ingress controller


Automatizace CI/CD


API Management

Podpora všech veřejných Cloudů

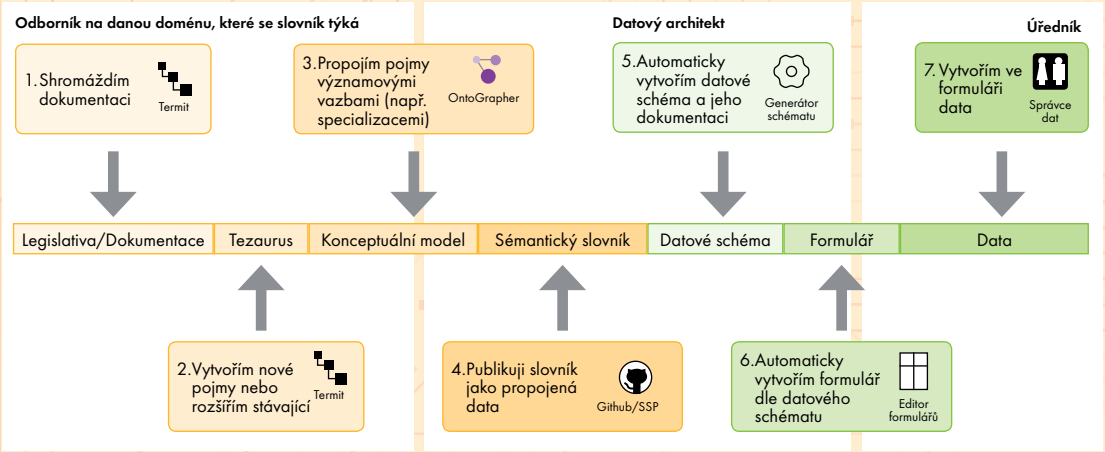

Podpora hybridního cloudu


Managed Kubernetes

Distributed Cloud Services

NGINX
Part of F5

Přehledový rámec tvorby a využití sémantického slovníku



Vytvořené sémantické slovníky (tezaury a konceptuální modely) nabízejí široké využití:

- získání podkladů pro kvalitní a úplnou evidenci údajů subjektů a objektů práva při ohlašování agendy v registru práv a povinností, včetně jejich významů s odkazy na legislativu a identifikovanými významovými vazbami mezi pojmy;
- automatické generování datových schémat otevřených dat, nebo datových rozhraní ISVS či kontextů ISSS pro potřeby PPDF;
- usnadnění návrhu formulářů dle datového schématu pro zadávání dat;
- snadnou komunikaci prostřednictvím diagramů;
- automatické vytváření výkladových slovníků;
- vyhledávání vzájemných významových souvislostí mezi datovými sadami, schématy a rozhraními (funkční nadstavba nad Katalogem otevřených dat NKOD).

Tento článek vznikl v rámci projektu „Rozvoj datových politik v oblasti zlepšování kvality a interoperability dat veřejné správy" OPZ č. CZ.03.4.74/0.0/0.0/15_025/0013983, který zastřešuje odbor hlavního architekta eGovernmentu, Ministerstvo vnitra ČR.

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Problematika modelování agend a kvalita evidovaných informací v RPP je součástí projektu „Rozvoj datových politik v oblasti zlepšování kvality a interoperability dat veřejné správy", CZ.03.4.74/0.0/0.0/15_025/0013983. V jeho rámci vznikly pro tyto oblasti ucelené metodiky a podpůrné nástroje, podpořené vzdělávacími aktivitami a školeními.

Jedná se zejména o:

- metodiku pro definici údajů vedených v agendě;
- metodiku tvorby a údržby sémantického slovníku pojmů veřejné správy;
- výrobní linku s podpůrnými nástroji pro tvorbu a údržbu konceptuálních modelů;
- školení „Modelování významu dat ve veřejné správě".

Konkrétní informace jsou dostupné na Portálu otevřených dat (data.gov.cz).

Modelování agend (tvorba a správa sémantických slovníků) představuje optimální způsob zajištění sémantické interoperability dat v prostředí veřejné správy. Má navíc potenciál výrazně ovlivnit kvalitu údajů veřejné správy, jejich evidenci, správu, jejich sdílení a všeobecné využití, a tak výrazně přispět k budování e-governmentu ČR v duchu deklarací zveřejněných v prohlášení vlády ČR.

Drahomír Chocholatý

Atos

Spolehněte se na **Atos,** skutečného experta na migraci **SAP.**

Komplexní zabezpečení řešení od **infrastruktury, implementace** až po **podporu.**

SAP Platinum Partner

#RISEwithSAP

O CO SE JEDNÁ

Egovernment The Best 2022 je soutěžní sbírka nejzajímavějších projektů elektronizace veřejné správy v ČR kterou každoročně, už 17 let, vyhlašuje Magazín Egovernment.

Snahou magazínu Egovernment je touto cestou shromáždit a prezentovat projekty, které byly (případně právě jsou) v rámci státní a veřejné správy v daném roce realizovány a mohou být inspirativní ostatním. Jednotlivé projekty mezi sebou soutěží v rámci **několika kategorií**.

Projekty můžete do soutěže přihlašovat pomocí elektronického formuláře. Uzávěrka přihlášek je 3. 11. 2022.

V polovině prosince bude všechny vydána publikace Egovernment The Best, která představuje všechny přihlášené projekty.

SOUTĚŽNÍ KATEGORIE

Přihlášené projekty jsou vzájemně porovnávány v těchto kategoriích (dle jejich charakteru):

- centrální projekty (realizované centrálními instutcemi, nebo projekty s celorepublikovým dosahem)
- krajské projekty
- městské projekty (města a MČ)
- obecní projekty (obce)

Jsou tak navzájem porovnávány pouze projekty adekvátního rozsahu a významu.

Cílem této kategorizace je odstranit obavy provozovatelů že jejich menší projekty nemohou uspět vedle velkých celostátních projektů.

JAK PŘIHLÁSIT PROJEKT?

Projekt může přihlásit kdokoliv - realizátor, provozovatel, spokojený uživatel... Může se tedy jednat o představitele úřadu či firma, ale rovněž o referenta, který má danou agendu na starosti a považuje projekt za přínosný, občana, kterému projekt pomohl atp.

Důležité je, že vybíráme pouze z projektů, které BUDOU PŘIHLÁŠENY. To znamená, pokud nezašlete přihlášku, příslušný projekt nebude do publikace zařazem a nemůže soutěžit!

Projekty můžete do soutěže přihlašovat **pomocí elektronického formuláře** na webových stránkách Magazínu Egovernnment.

PRINCIP

Princip **Egovernment The Best** je tedy v tom, že přihlásíte projekt ve Vašem okolí, který směřuje k elektronizaci veřejné správy a který považujete za přínosný.

Projekt je následně zařazen do příslušné kategorie a porovnáván/ hodnocen pouze ve vztahu k projektům obdobného charakteru či velikosti.

VŠECHNY projekty, které budou přihlášeny, budou prezentovány na webových stránkách Magazínu Egovernment a následně v publikaci Egovernment The Best 2022.

V rámci jednotlivých kategorií budou vyhlášeny vždy tři nejzajímavější projekty.

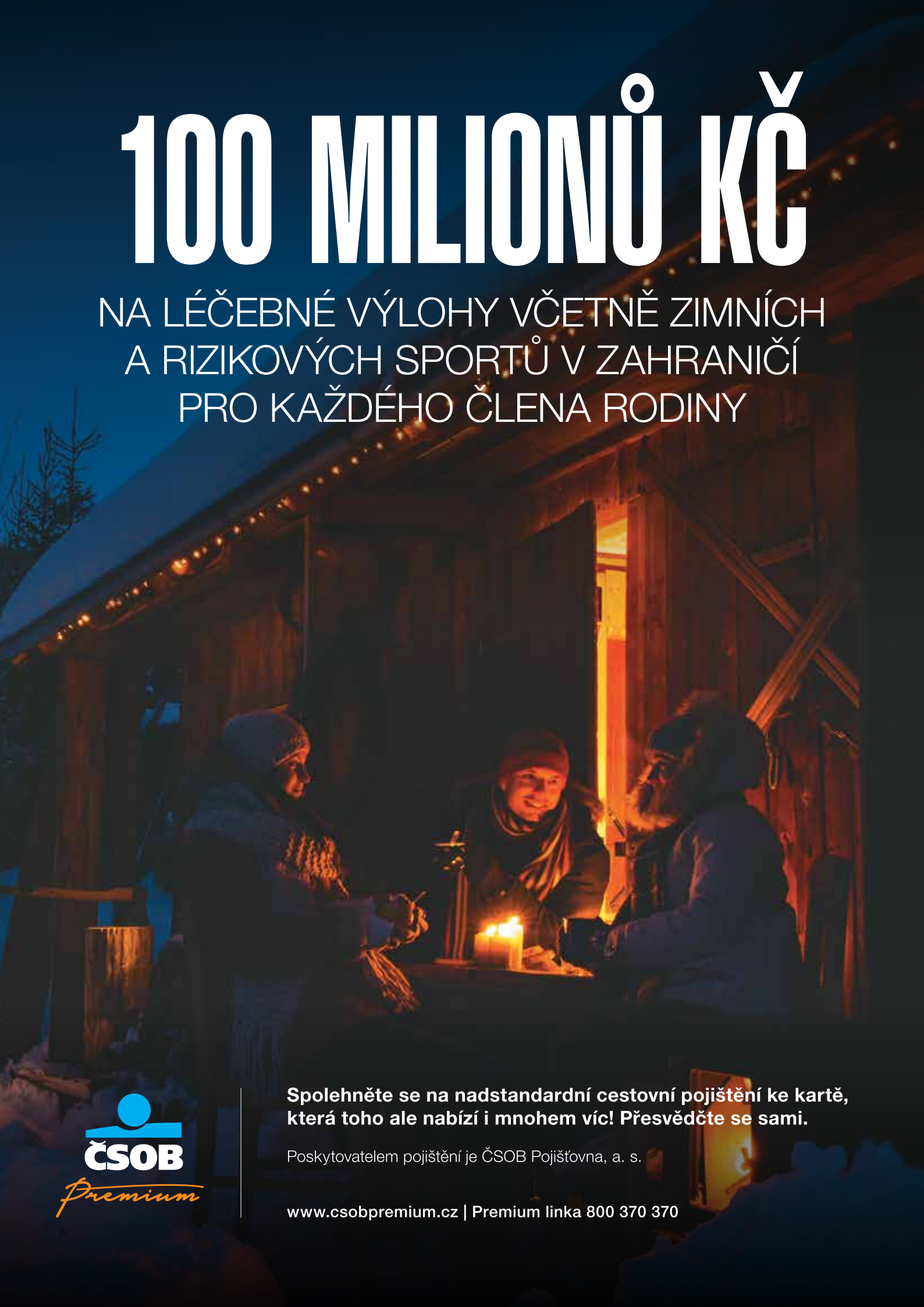
Egovernment
elektronizace veřejné správy

THE BEST 2022

ICZ

Projekty elektronizace můžete do letošního ročníku přihlašovat na **www.egovernment.cz**.

Uzávěrka přihlášek je **3. 11. 2022**


100 MILIONŮ KČ
NA LÉČEBNÉ VÝLOHY VČETNĚ ZIMNÍCH
A RIZIKOVÝCH SPORTŮ V ZAHRANIČÍ
PRO KAŽDÉHO ČLENA RODINY
ČSOB
Premium
Spolehněte se na nadstandardní cestovní pojištění ke kartě,
která toho ale nabízí i mnohem víc! Přesvědčte se sami.
Poskytovatelem pojištění je ČSOB Pojišťovna, a. s.
www.csobpremium.cz | Premium linka 800 370 370